



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Φαίδρας Κωνσταντίου (Α.Μ.: ΜΔΙ 2222)

**ΜΕΤΑΔΕΔΟΜΕΝΑ ΚΑΙ ΑΠΟΡΡΗΤΟ ΕΠΙΚΟΙΝΩΝΙΩΝ ΣΤΑ ΣΥΣΤΗΜΑΤΑ
ΜΑΖΙΚΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΑΙ ΔΙΑΤΗΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ:
ΜΙΑ ΜΕΛΕΤΗ ΤΟΥ ΚΑΝΟΝΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΕΕ-ΕΛΛΑΔΑΣ**

**METADATA AND PRIVACY OF COMMUNICATIONS IN MASS
SURVEILLANCE AND DATA RETENTION SYSTEMS:
A STUDY OF THE EU-GREEK REGULATORY FRAMEWORK**

Επιβλέπουσα:

Δρ. Αικατερίνα Παπανικολάου

Πειραιάς, Νοέμβριος 2024

Περιεχόμενα

Περίληψη	4
Summary.....	5
Εισαγωγή	5
1. Η «επικοινωνία» ως έννοια.....	7
1.1 Θεωρητικές προσεγγίσεις για το περιεχόμενο, το νόημα και την σημασία	7
2. Η έννοια των «μεταδεδομένων της επικοινωνίας»	13
2.1 Κατηγορίες μεταδεδομένων	16
2.2. Περιπτώσεις χρήσης των μεταδεδομένων της επικοινωνίας.....	18
2.2.1 Παρακολούθηση στο πλαίσιο της επιβολής του νόμου	18
2.3. Ανάλυση των όρων «εξωτερικά στοιχεία της επικοινωνίας» και «μεταδεδομένα».....	21
3. Η κατοχύρωση του δικαιώματος του απορρήτου της επικοινωνίας σε διεθνές επίπεδο ...	22
3.1 Διεθνή κείμενα	23
3.2 Άρθρο 8 ΕΣΔΑ.....	23
3.3 Περιορισμοί του άρθρου 8 ΕΣΔΑ	25
4. Κατοχύρωση της προστασίας του απορρήτου της επικοινωνίας σε Ευρωπαϊκό επίπεδο .	25
4.1. Παράγωγο δίκαιο της ΕΕ.....	26
4.2 Οδηγία 2002/58/ΕΚ (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες -E Privacy Directive)	27
4.3 Η Οδηγία 2006/24/ΕΚ (Data Retention Directive).....	28
4.4 Πρόταση για τον Κανονισμό e-Privacy.....	30
4.5 Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ-GDPR).....	31
5. Νομολογιακή Επισκόπηση σε Ευρωπαϊκό επίπεδο.....	32
5.1 Αποφάσεις ΕΔΔΑ	32
5.1.1 Malone κατά Ηνωμένου Βασιλείου	32
5.1.2 Roman Zakharov κατά Ρωσίας	33
5.1.3 Szabó και Vissy κατά Ουγγαρίας	34
5.1.4 Centrum för Rättvisa κατά Σουηδίας	37
5.1.5 Big Brothers Watch and Others κατά Ηνωμένου Βασιλείου.....	38
5.1.6. Οι αποφάσεις του τμήματος Μείζονος Συνθέσεως για την υπόθεση Big Brother Watch κατά του Ηνωμένου Βασιλείου και Centrum för Rättvisa κατά Σουηδίας	40
5.1.7 Benedik κατά Σλοβενίας.....	41
5.1.8. Breyer κατά Γερμανίας.....	43

5.1.8 Ekimdziev και άλλοι κατά Βουλγαρίας	45
5.1.9 Pietrzak και άλλοι κατά Πολωνίας.....	46
5.2 Νομολογία ΔΕΕ	49
5.2.1 Απόφαση Digital Rights Ireland και άλλοι.....	49
5.2.2 Tele2 Sverige AB κατά Post-och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis	50
5.2.3 Prokuratuur C-746/18	52
5.2.4 Joined Cases C-339/20 (VD) and C-397/20(SR) και Joined Cases C-793/19 (SpaceNet) and C-794/19 (Telekom Deutschland).....	54
5.3. Ευρωπαϊκή νομολογία και μαζική παρακολούθηση	56
5.3.1 Σύγκριση νομολογίας ΕΔΔΑ και ΔΕΕ.....	56
5.3.2. Η θέση της ευρωπαϊκής νομολογίας για την μαζική παρακολούθηση και την γενική διατήρηση μεταδεδομένων	57
6. Τα μεταδεδομένα επικοινωνίας στην ελληνική έννομη τάξη	58
6.1 Άρθρο 19 του Συντάγματος	59
6.2 Μεταδεδομένα της επικοινωνίας και απόρρητο	60
7. Ανάλυση και κριτική του νόμου 5002/2022	62
7.1 Εξωτερικά στοιχεία της επικοινωνίας.....	62
7.2 Λόγοι «εθνικής ασφάλειας»	64
7.3 Άρση για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.....	69
7.4 Διαδικασία άρσης του απορρήτου.....	71
7.5 Γνωμοδότηση 1/2023- « Ερμηνεία του Ν. 5002/2022 «Διαδικασία άρσης απορρήτου επικοινωνιών, κυβερνοασφάλεια, προστασία προσωπικών δεδομένων πολιτών»	72
7.6 Συμπέρασμα κριτικής νόμου.....	74
8. Νομολογιακό παράδειγμα στο νέο νομικό πλαίσιο.....	77
8.1 Το ιστορικό του «σκανδάλου των υποκλοπών» στην Ελλάδα	77
8.2 Απόφαση 465/2024 ΣτΕ	82
8.2.1. Δικαίωμα «γνωστοποίησης».....	82
8.2.3 Ο όρος «εθνική ασφάλεια» και η επέμβασή του στο δικαίωμα	84
8.2.3. Συμμόρφωση της Διοίκησης και χρονική ισχύς νόμου	85
Συμπέρασμα	87
Βιβλιογραφία	89
1. Ξενόγλωσση βιβλιογραφία-αρθρογραφία	89
2. Ελληνική βιβλιογραφία-αρθρογραφία	90
3. Κανονισμοί και Οδηγίες της ΕΕ	93

4. Αποφάσεις ΕΔΔΑ.....	93
5. Αποφάσεις ΔΕΕ.....	94
6. Ιστοσελίδες-Blog.....	94
7. Δελτία τύπου ΑΔΑΕ.....	95
8. Γνωμοδοτήσεις.....	95
9. Διεθνή κείμενα	96
10. Podcast.....	96

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τη νομική προστασία του απορρήτου των επικοινωνιών, με έμφαση στα μεταδεδομένα επικοινωνίας, ως ουσιώδες μέρος του προστατευτέου απορρήτου. Η ανάλυση αναδεικνύει τη σημασία των μεταδεδομένων, τα οποία, αν και δεν περιέχουν το περιεχόμενο των επικοινωνιών, παρέχουν εξίσου αποκαλυπτικές πληροφορίες για τις σχέσεις και τις δραστηριότητες των ατόμων. Στο πλαίσιο αυτό, τίθενται κρίσιμα ερωτήματα, σχετικά με την επάρκεια των θεσμικών εγγυήσεων που προβλέπονται, τόσο από την ελληνική έννομη τάξη όσο και από την ευρωπαϊκή νομολογία.

Η εργασία εξετάζει διεξοδικά το ισχύον νομικό πλαίσιο σε διεθνές και ευρωπαϊκό επίπεδο, με έμφαση στη νομολογία του ΕΔΔΑ και του ΔΕΕ, ιδίως στις αποφάσεις που αφορούν τη μαζική παρακολούθηση και τη γενική διατήρηση δεδομένων. Οι αποφάσεις αυτές αναδεικνύουν τα όρια της κρατικής επέμβασης, θέτοντας αυστηρές προϋποθέσεις για τη διασφάλιση της αναλογικότητας, της νομιμότητας και της ύπαρξης επαρκών εγγυήσεων.

Στη συνέχεια, η εργασία στρέφεται στο ελληνικό νομικό πλαίσιο, με κεντρικό άξονα τον νόμο 5002/2022, ο οποίος εισήγαγε σημαντικές αλλαγές στη διαδικασία άρσης του απορρήτου των επικοινωνιών. Μέσα από την ανάλυση της νομολογίας και των θεσμικών διατάξεων, καθώς και με αναφορά στην πρόσφατη «υπόθεση των υποκλοπών», εξετάζονται τα δικαιώματα των θιγόμενων πολιτών καθώς και η συνταγματικότητα των ρυθμίσεων. Η συσχέτιση των ελληνικών πρακτικών με τα πρότυπα που θέτουν τα ευρωπαϊκά δικαστήρια αποκαλύπτει ανεπάρκειες στις θεσμικές εγγυήσεις, τόσο ως προς την πρόληψη καταχρηστικών παρακολουθήσεων, όσο και ως προς τη λογοδοσία των κρατικών αρχών.

Η εργασία καταλήγει στο συμπέρασμα ότι οι ισχύουσες θεσμικές εγγυήσεις, σε ευρωπαϊκό και εθνικό επίπεδο, δεν επαρκούν για την πλήρη προστασία του απορρήτου των επικοινωνιών. Παρά τη νομολογιακή πρόοδο και την ύπαρξη νομοθετικών ρυθμίσεων, συνεχίζουν να υπάρχουν κενά προστασίας, που υπονομεύουν το δικαίωμα στην ιδιωτικότητα. Μέσα από την κριτική αποτίμηση των νομικών και θεσμικών πλαισίων, αναδεικνύεται η ανάγκη περαιτέρω ενίσχυσης των εγγυήσεων, ώστε να αντιμετωπιστούν οι σύγχρονες προκλήσεις και να διασφαλιστεί αποτελεσματικά το δικαίωμα στην ιδιωτικότητα των ατόμων.

Summary

This thesis examines the legal protection of communications privacy, with a focus on communication metadata as an essential part of protectable communications privacy. The analysis highlights the importance of metadata. Although the research does not include the content of communications, it provides equally revealing information about the relationships and activities of individuals. In this context, critical questions are raised in regard to the adequacy of the institutional guarantees provided by both Greek law and European case law.

The paper thoroughly examines the current legal framework at international and European level, with an emphasis on the case law of the ECtHR and the CJEU. In particular the thesis discusses the decisions concerning mass surveillance and general data retention. These judgments highlight the limits of state intervention, while setting strict conditions to ensure proportionality, legality and the existence of adequate safeguards.

The research then turns to the Greek legal framework, focusing on Law 5002/2022, which introduced significant changes to the procedure of lifting the confidentiality of communications. Through the analysis of case law, institutional provisions, and the recent case of the "wiretapping scandal", the rights of affected citizens and the constitutionality of the regulations are examined. The comparison of Greek practices with the standards set by European courts reveals inadequacies in institutional guarantees when it comes to the prevention of arbitrary interception as well as the accountability of state authorities.

The thesis concludes that the existing institutional safeguards, at European and national level, are not sufficient to fully protect the confidentiality of communications. Despite legislative progress and the existence of legal provisions, there are still gaps when it comes to the

protection of the right to privacy. A critical assessment of the legal and institutional frameworks highlights the need to further strengthen safeguards to address contemporary challenges and effectively ensure the privacy of individuals.

Εισαγωγή

Η έννοια του απορρήτου των επικοινωνιών αποτελεί έναν από τους θεμελιώδεις πυλώνες προστασίας των ατομικών δικαιωμάτων σε ένα σύγχρονο δημοκρατικό κράτος δικαίου. Ωστόσο, η τεχνολογική εξέλιξη και η αυξανόμενη ψηφιοποίηση της επικοινωνίας έχει οδηγήσει στην συλλογή και διατήρηση μεταδεδομένων επικοινωνίας, μάλιστα μερικές φορές γενικού χαρακτήρα, γι' αυτό και διαδραματίζουν καίριο ρόλο στα συστήματα επιτήρησης που εφαρμόζονται από κρατικές αρχές και υπηρεσίες επιβολής του νόμου. Αποτελούν, επίσης, εργαλείο για την κατάρτιση προφίλ των πολιτών, μέσω της αναγνώρισης προτύπων συμπεριφοράς και σχέσεων που επιτρέπουν την εκτίμηση μελλοντικών ενεργειών. Αυτή η δυνατότητα των αρχών να αποκτούν ενδελεχή γνώση για τη ζωή των πολιτών, ακόμη και χωρίς πρόσβαση στο περιεχόμενο των συνομιλιών, εγείρει σοβαρά ζητήματα για την προστασία της ιδιωτικότητας σε σχέση με τα όρια της κρατικής επέμβασης.

Κρίσιμης σημασίας στην ανάλυση της παρούσας διπλωματικής εργασίας είναι η διερεύνηση του ισχύοντος νομικού πλαισίου στην Ευρωπαϊκή Ένωση και η νομολογία των ευρωπαϊκών δικαστηρίων, κυρίως του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) και του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), τα οποία ερμηνεύουν τα βασικά κείμενα που προστατεύουν την ιδιωτικότητα των επικοινωνιών στην ΕΕ, δηλαδή την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) και τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Ωστόσο, με την αυξανόμενη χρήση τεχνολογιών παρακολούθησης και τη γενική διατήρηση μεταδεδομένων, τα δικαστήρια αυτά έχουν κληθεί να καθορίσουν τις προϋποθέσεις και τους περιορισμούς της κρατικής επέμβασης στην ιδιωτική σφαίρα των πολιτών.

Η σημασία της ανάλυσης έγκειται στο γεγονός, ότι οι αποφάσεις αυτές διαμορφώνουν μια κοινή ευρωπαϊκή στάση απέναντι στα συστήματα μαζικής παρακολούθησης και υποδεικνύουν την κατεύθυνση προς την οποία κινείται η ευρωπαϊκή νομολογία, αναφορικά με αυτό. Μέσω αυτής της εξέτασης, μπορούμε να κατανοήσουμε τις νομικές και

θεσμικές απαιτήσεις που επιβάλλουν τα ευρωπαϊκά δικαστήρια στα κράτη-μέλη, ώστε να διασφαλίζεται η προστασία του απορρήτου των επικοινωνιών.

Στο τρίτο μέρος της διπλωματικής εργασίας, η ανάλυση επικεντρώνεται στο ελληνικό νομικό πλαίσιο γύρω από την άρση του απορρήτου των επικοινωνιών και τον ρόλο των μεταδεδομένων στη διαδικασία αυτή. Ο νόμος 5002/2022 για τις άρσεις του απορρήτου εισάγει σημαντικές αλλαγές, ιδίως στο πλαίσιο που αφορά τα μεταδεδομένα επικοινωνίας καθώς και το δικαίωμα ενημέρωσης των θιγόμενων πολιτών. Η ψήφιση αυτού του νόμου συνδέεται στενά με την πρόσφατη «υπόθεση των υποκλοπών», η οποία επανέφερε στο προσκήνιο την ανάγκη για ενίσχυση των θεσμικών εγγυήσεων που αποτρέπουν την κατάχρηση των παρακολουθήσεων. Σημαντικά ζητήματα προς διερεύνηση είναι η συνταγματικότητα των διατάξεων του νόμου, οι θεσμικές εγγυήσεις αυτού και η εναρμόνισή του με τη νομολογία των ευρωπαϊκών δικαστηρίων.

Εξετάζοντας το νομικό πλαίσιο και τις πρακτικές που ακολουθούνται στην Ελλάδα, θα αποτιμηθεί κατά πόσο το υπάρχον σύστημα προστασίας του απορρήτου των επικοινωνιών πληροί τις απαιτήσεις που θέτει το ενωσιακό δίκαιο και η νομολογία του ΕΔΔΑ και του ΔΕΕ. Η ανάλυση αυτή θα συμβάλλει στην κατανόηση του πραγματικού επιπέδου προστασίας της ιδιωτικότητας στη χώρα μας και θα αναδείξει τυχόν αδυναμίες του νομικού συστήματος.

Καθώς τα όρια μεταξύ προστασίας και παρακολούθησης γίνονται ολοένα πιο ασαφή, η ανάγκη για σαφείς προστατευτικές εγγυήσεις και σεβασμό των δικαιωμάτων του ατόμου παραμένει πιο επιτακτική από ποτέ. Το ερώτημα που τίθεται δεν είναι απλώς νομικό, αλλά βαθιά ανθρωπινό: ποια είναι η αξία της ιδιωτικότητας σ' έναν κόσμο όπου όλα καταγράφονται χωρίς να ειπωθούν.

1.Η «επικοινωνία» ως έννοια

1.1 Θεωρητικές προσεγγίσεις για το περιεχόμενο, το νόημα και την σημασία

Εξερευνώντας την εξελικτική πορεία των σπουδών επικοινωνίας από τον 20ό αιώνα και έπειτα, παρατηρούμε ένα πλούσιο φάσμα επιστημονικών επιρροών που διαμορφώνουν κομβικά ερευνητικά έργα και θεωρητικά πλαίσια στο πεδίο αυτό. Σε αυτό το εισαγωγικό τμήμα, θα επιχειρηθεί μία σύντομη αναδρομή στις επιστημολογικές ρίζες των

επικοινωνιακών σπουδών, ορίζοντας θεμελιώδεις έννοιες, όπως η ίδια η «επικοινωνία». Στο πλαίσιο της αναζήτησης του τι είναι επικοινωνία, γίνεται προσπάθεια να αναδειχθούν οι τυπικοί ρόλοι και οι κοινωνικοί φορείς που εμπλέκονται στις διάφορες επικοινωνιακές διαδικασίες και οι σχέσεις που διαμορφώνονται μέσω της επικοινωνίας. Η προσέγγιση έχει στόχο να αναδείξει την πολύπλευρη φύση του θέματος, ενώ τονίζει τη διεπιστημονική ουσία της φύσης της επικοινωνίας, συστατικό στοιχείο της οποίας είναι και τα μεταδεδομένα.

Ένας από τους πρώτους θεωρητικούς, ο Charles Cooley¹, παρατήρησε ότι η επικοινωνία περιλαμβάνει μια μετάβαση από μια οργανωμένη κατάσταση σε μια άλλη, με βελτιωμένη δομή². Μία από τις θεωρίες του περιλαμβάνει την ιδέα, ότι η επικοινωνία είναι ο μηχανισμός άσκησης της εξουσίας. Ο Cooley δίνει έμφαση στο «ποιος», «πότε» και «πώς» επικοινωνεί με γνώμονα την απόκτηση της εξουσίας. Στο ίδιο μοτίβο σκέψης εισάγει την έννοια της «συμμετρικής επικοινωνίας»³, δηλαδή όταν εντοπίζεται αμφίδρομη και ίση συχνότητα στην διαμοιβή μηνυμάτων επικοινωνίας (πχ σε έναν διάλογο). Η σημασία της παρατήρησης αυτής έγκειται στον ρόλο που διαδραματίζει, εν τέλει, η επικοινωνία και οι μορφές της στο πλαίσιο της κοινωνίας και των δικαιωμάτων. Η «συμμετρία των αμφίδρομων ανταλλαγών», όπως την έθεσε ο Cooley, συμβάλλει στην εκδημοκρατικοποίηση των συνθηκών, καλλιεργώντας μια πολιτική κουλτούρα με γνώμονα την μη καταπάτηση των ατομικών δικαιωμάτων. Η «επικοινωνιακή συμμετρικότητα», κατ' επέκταση, λειτουργεί ως βάση για την κατοχύρωση της «ελευθερίας της έκφρασης», ως ατομικό δικαίωμα.

Σύμφωνα με τον John Fiske⁴, η επικοινωνία είναι ένα διεπιστημονικό πεδίο στο οποίο δεν μπορούν να εφαρμοστούν καθολικές και απόλυτες θεωρίες. Πολλοί διαφορετικοί επιστημονικοί κλάδοι έχουν επικεντρωθεί στην μελέτη πολλαπλών πτυχών της

¹ (Cooley, 1998) Διαθέσιμο σε: <https://books.google.gr/books?id=Duzk5w-MOR0C&printsec=frontcover#v=onepage&q&f=false>

² Η επικοινωνία περιλαμβάνει όλα τα σύμβολα του νου, μαζί με τα μέσα μετάδοσής τους στο χώρο και διατήρησής τους στο χρόνο. Περιλαμβάνει την έκφραση του προσώπου, τη στάση και τις χειρονομίες, τους τόνους της φωνής, τις λέξεις, τη γραφή, την τυπογραφία, τους σιδηρόδρομους, τον τηλεγράφο, το τηλέφωνο και οποιοδήποτε άλλο πρόσφατο επίτευγμα, στην πορεία για την κατάκτηση του χώρου και του χρόνου.

³ (Cooley, 1998)

⁴ (Fiske, 2011)

επικοινωνίας. Ο Fiske προχωράει σε μερικές εισαγωγικές παραδοχές: αρχικά, θεωρεί ότι η επικοινωνία μπορεί να μελετηθεί συστηματικά σαν επιστημονικό αντικείμενο και περιλαμβάνει τη χρήση σημείων, τα οποία μεταφέρουν νοήματα πέρα από την κυριολεκτική τους έννοια (μπορεί να περιλαμβάνουν γλώσσα, χειρονομίες, εικόνες και άλλα). Αυτό ευθυγραμμίζεται με τη σημειωτική, τη μελέτη των σημείων, των συμβόλων και της χρήσης ή της ερμηνείας τους. Επιπλέον, τα σημεία αυτά ακολουθούν μοτίβα και μπορούν να γίνουν κατανοητά μέσω της έρευνας και της παρατήρησης και να οργανώνονται σε κώδικες, δηλαδή, σε συστήματα κανόνων και συμβάσεων που διέπουν τον τρόπο με τον οποίο χρησιμοποιούνται και ερμηνεύονται τα σημεία σε έναν συγκεκριμένο πολιτισμό ή κοινωνικό πλαίσιο. Για παράδειγμα, η ίδια η γλώσσα είναι ένας κώδικας με κανόνες για τη γραμματική, το συντακτικό και τη σημασιολογία.

Ο Fiske θεωρεί την επικοινωνία ως κοινωνική πρακτική⁵, πράγμα που σημαίνει ότι η μετάδοση των σημείων είναι βαθιά ενσωματωμένη στις κοινωνικές σχέσεις και τα πολιτισμικά πλαίσια. Η επικοινωνία δεν μεταδίδει απλώς πληροφορίες· ενισχύει, ταυτόχρονα, κοινωνικούς κανόνες, ταυτότητες και δομές εξουσίας. Ισχυρίζεται, ότι η επικοινωνία είναι κεντρική κοινωνική πρακτική για τον πολιτισμό, πράγμα που σημαίνει, ότι διαδραματίζει θεμελιώδη ρόλο στη διαμόρφωση και τη διατήρηση πολιτισμικών πρακτικών, πεποιθήσεων και αξιών. Μέσω της επικοινωνίας, τα άτομα κατασκευάζουν και διαπραγματεύονται την κατανόηση του κόσμου, καθώς και τις ταυτότητές τους μέσα σε αυτόν. Αυτές οι υποθέσεις διαμορφώνουν συλλογικά ένα πλαίσιο για την κατανόηση της επικοινωνίας, ως μιας πολύπλευρης διαδικασίας, που διαμορφώνεται και διαμορφώνει τις κοινωνικές αλληλεπιδράσεις και τις πολιτισμικές δυναμικές, καταλήγοντας και σε κοινές πεποιθήσεις. Οι υποθέσεις του Fiske για την επικοινωνία έχουν βαθιές ρίζες στην θεώρηση, ότι η επικοινωνία δεν είναι απλώς η ανταλλαγή πληροφοριών, αλλά μια σύνθετη διαδικασία συνυφασμένη με την κοινωνική και πολιτισμική αλληλεπίδραση.

Στην μελέτη του για την ανάλυση της επικοινωνίας, ο Fiske ασχολήθηκε με 2 σχολές-προσεγγίσεις: την σχολή της «επεξεργασίας» (process school) και την σχολή της «σημειωτικής» (semiotics school)⁶. Η πρώτη, επικεντρώνεται στον τρόπο με τον οποίο τα μηνύματα μεταδίδονται από το ένα άτομο στο άλλο, θεωρώντας την επικοινωνία ως την

⁵ (Tomszewski, 2003) Διαθέσιμο σε: <http://zach.tomaszewski.name/uh/cis701/paper4.html>

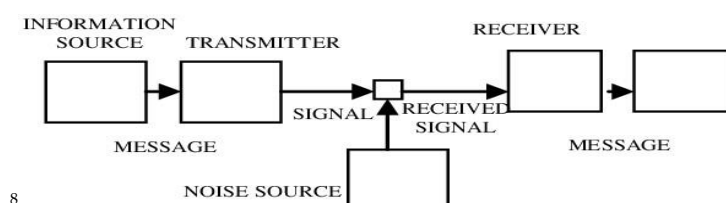
⁶ (Fiske, 2011)

πράξη με την οποία επηρεάζονται οι σκέψεις ή οι ενέργειες του πομπού και του αποδέκτη της επικοινωνίας. Η δεύτερη προσέγγιση, δίνει έμφαση στην ερμηνεία του νοήματος, δίνοντας προσοχή στα σήματα που ανταλλάσσονται μεταξύ αποστολέα και παραλήπτη και στο πολιτισμικό πλαίσιο μέσα στο οποίο διαμορφώνεται το νόημά τους⁷.

Σημαντικό κομμάτι της σχολής της επεξεργασίας αποτελεί το μοντέλο των Shannon και Weaver του 1948⁸. Το μοντέλο αυτό δεν εμβαθύνει πολύ στο ρόλο του νοήματος και της κουλτούρας, υποθέτοντας ότι το μήνυμα φέρει εγγενώς το νόημά του⁹. Πρόκειται για την περιγραφή της επικοινωνίας ως μιας γραμμικής διαδικασίας από την πηγή στον πομπό, μέσω ενός καναλιού, στον δέκτη. Πάνω στο μοντέλο των Shannon και Weaver βασίστηκαν και εξελίχθηκαν άλλα μοντέλα διεργασιών που ανήκαν στην λογική της σχολής της «επεξεργασίας».

Η σημειωτική σχολή σε αντίθεση με τις υπόλοιπες προσεγγίσεις¹⁰, εστιάζει στο πώς δημιουργείται το νόημα μέσω της αλληλεπίδρασης μεταξύ του αποστολέα και του μηνύματος ή του δέκτη και του μηνύματος. Η σημειωτική αναλύει τα ίδια τα σημεία, τους κώδικες ή τα συστήματα στα οποία είναι δομημένα τα σημεία και ταυτόχρονα το πολιτισμικό πλαίσιο στο οποίο λειτουργούν αυτοί οι κώδικες. Ο γλωσσολόγος Ferdinand de Saussure τονίζει τη σημασία του ίδιου του σημείου. Θεωρεί ότι το σημείο αποτελείται από δύο μέρη: το σημαίνον, που είναι η φυσική μορφή του σημείου (όπως οι προφορικοί ήχοι ή τα γραπτά γράμματα), και το σημαινόμενο, που είναι η νοητική έννοια ή ιδέα στην οποία αναφέρεται το σημείο. Σύμφωνα με τον Saussure, το νόημα ενός σημαινόμενου

⁷ (Tomszewski, 2003)



⁸ (Al-Fedaghi,

2012):

Διαθέσιμο

σε:

https://www.researchgate.net/publication/272964534_A_Conceptual_Foundation_for_the_Shannon-Weaver_Model_of_Communication

¹⁰ (Fiske, 2011)

καθορίζεται περισσότερο από το σύστημα των σημαινόντων, από τα όρια και τις σχέσεις μεταξύ αυτών και πρόκειται για μία δυναμική διαδικασία και όχι απόλυτη και σταθερή¹¹.

Η ανάλυση της έννοιας της επικοινωνίας από αυτή την οπτική γωνία, προσφέρει μια πολύτιμη εικόνα της δυναμικής φύσης της επικοινωνίας ως μοντέλου. Εξετάζοντας τις διάφορες πτυχές της, συμπεριλαμβανομένης της μετάδοσης μηνυμάτων, της παραγωγής νοήματος και της χρήσης κωδίκων και σημαινομένων, αποκτούμε βαθύτερη κατανόηση του τρόπου με τον οποίο η επικοινωνία λειτουργεί μέσα σε κοινωνικά και πολιτισμικά πλαίσια. Η προσέγγιση αυτή τονίζει ότι η επικοινωνία δεν είναι μια στατική διαδικασία, αλλά, μια δυναμική αλληλεπίδραση μεταξύ των ατόμων, των μηνυμάτων τους και των πολιτισμικών συστημάτων στα οποία λειτουργούν. Υπογραμμίζει τη σημασία της διερεύνησης, όχι μόνο του τι λέγεται, αλλά και του τρόπου με τον οποίο ερμηνεύεται, καθώς και των πολιτισμικών παραγόντων που διαμορφώνουν αυτές τις ερμηνείες. Μέσω αυτού του φακού, η επικοινωνία αναδεικνύεται ως ένα σύνθετο και πολύπλευρο φαινόμενο, ζωτικής σημασίας για την κατανόηση της ανθρώπινης αλληλεπίδρασης και της κοινωνικής δυναμικής.

Ο Charles Cooley και ο John Fiske προσφέρουν συμπληρωματικές γνώσεις, σχετικά με τη δυναμική της επικοινωνίας και της εξουσίας. Η παρατήρηση του Cooley, ότι η επικοινωνία χρησιμεύει ως μηχανισμός άσκησης εξουσίας, υπογραμμίζει τον κρίσιμο ρόλο της στη διαμόρφωση των κοινωνικών σχέσεων και της δυναμικής της εξουσίας. Επισημαίνει τη σημασία του ποιος επικοινωνεί, πότε και πώς, υπογραμμίζοντας τον τρόπο με τον οποίο αυτοί οι παράγοντες προβλέπουν και επηρεάζουν τις σχέσεις εξουσίας. Ο Fiske, από την άλλη πλευρά, εμβαθύνει στις πολιτισμικές διαστάσεις της επικοινωνίας, δίνοντας έμφαση στον ρόλο της λαϊκής κουλτούρας στη διαμόρφωση των κοινωνικών κανόνων και ταυτοτήτων.

Η έννοια της «σημειωτικής δημοκρατίας» υπογραμμίζει τη δύναμη των απλών ανθρώπων στη διαμόρφωση του νοήματος και την αντίσταση στις κυρίαρχες πολιτισμικές αφηγήσεις. Ενώνοντας την έμφαση του Cooley στην άσκηση εξουσίας μέσω της επικοινωνίας, με την εστίαση του Fiske στην πολιτισμική δράση, αναγνωρίζουμε πώς η επικοινωνία τόσο αντανακλά όσο και διαμορφώνει τις δομές εξουσίας, ενώ παράλληλα αναγνωρίζουμε τη

¹¹ (Tomszewski, 2003)

δυνατότητα των ατόμων και των κοινοτήτων να αμφισβητούν και να αναδιαμορφώνουν αυτές τις δομές μέσω των επικοινωνιακών τους πρακτικών.

Στην ελληνική θεωρία η επικοινωνία έχει οριστεί ως επικοινωνία με «στενή έννοια» και επικοινωνία με «ευρεία έννοια». Ως επικοινωνία με την στενή έννοια ορίζεται «η μετάδοση συγκεκριμένων ανθρώπινων στοχασμών, η μεταβίβαση (διαβίβαση) μηνύματος με προσδιορισμένο περιεχόμενο μεταξύ αυτών που επικοινωνούν», ενώ ως επικοινωνία με ευρεία έννοια ορίζεται «κάθε ανθρώπινη σχέση», πρόκειται δηλαδή για μια επικοινωνία που δεν έχει απαραίτητα ένα καθορισμένο περιεχόμενο. Τα βασικά στοιχεία της επικοινωνίας, με βάση το γραμμικό μοντέλο των Shannon και Weaver, όπως αναφέρθηκε ανωτέρω και την «σχολή της επεξεργασίας» είναι τα υποκείμενα τα οποία επικοινωνούν και το ίδιο το μεταβιβαζόμενο μήνυμα¹².

Οι επικοινωνούντες διακρίνονται, περαιτέρω, στον αποστολέα-πομπό και στον δέκτη του μηνύματος. Το μεταβιβαζόμενο μήνυμα, λαμβάνει διάφορες μορφές, από προφορικές συνομιλίες και γραπτές επιστολές έως οπτικές εικόνες και ηλεκτρονικά δεδομένα, αντανακλώντας την ευελιξία της ανθρώπινης επικοινωνίας. Οποιαδήποτε μορφή, όμως και αν έχει, αντανακλά την ανθρώπινη σκέψη και πρόθεση. Οι μέθοδοι επικοινωνίας μας, είτε μέσω συνομιλίας, ραδιοφώνου, επιστολών, τηλεόρασης ή οποιουδήποτε άλλου μέσου, όλες διαμορφώνονται από την ανθρώπινη σκέψη και πρόθεση.

Τα δευτερεύοντα στοιχεία της επικοινωνίας είναι το σήμα, το κανάλι, το μέσο και ο μεταδότης-δέκτης. Το σήμα είναι ο τρόπος μετάδοσης του μηνύματος, που επιτρέπει τη μετάδοσή του. Το κανάλι είναι η δίοδος μεταβίβασης του σήματος μεταξύ των επικοινωνούντων. Το μέσο διακρίνεται σε μέσο εν ευρεία έννοια, όπου πρόκειται για «τον τεχνικό ή φυσικό τρόπο μετατροπής του μηνύματος σε σήμα ικανό να μεταδοθεί από το κανάλι» και σε μέσο εν στενή έννοια, όπου εδώ εμπίπτει σε μέσα «παραστατικά», «αναπαραστατικά» και «μηχανικά»¹³.

Τέλος, μία σημαντική πτυχή της επικοινωνίας για την παρούσα εργασία, είναι η φύση της επικοινωνίας ως προς το μυστικό χαρακτήρα ή μη του περιεχομένου της. Επομένως, διακρίνεται σε «απόρρητη» επικοινωνία, όπου τα μέρη που επικοινωνούν, επιθυμούν να κρατήσουν την επικοινωνία μυστική από τρίτους δέκτες και σε «μη απόρρητη», όπου οι

¹² (Παπαδόπουλος, 2008, σελ. 2-3)

¹³ (Παπαδόπουλος, 2008)

επικοινωνούντες δεν έχουν σκοπό να διατηρήσουν μυστικό το περιεχόμενο της επικοινωνίας¹⁴.

2. Η έννοια των «μεταδεδομένων της επικοινωνίας»

Η έννοια των μεταδεδομένων της επικοινωνίας εμφανίστηκε στα τέλη της δεκαετίας του 1960, αλλά η καταγωγή του όρου μεταδεδομένα δεν είχε την ίδια σημασία με αυτή που έχει σήμερα. Επινοημένος το 1960, ο όρος μεταδεδομένα δεν εξεταζόταν στο πλαίσιο της πληροφορικής και των επικοινωνιών όπως συμβαίνει σήμερα. Η αλλαγή αυτή συνέβη τον Ιούνιο του 2013, με τις δημοσιεύσεις που βασίστηκαν στα έγγραφα που διέρρευσε ο Edward Snowden, αποκαλύπτοντας τα συστήματα συλλογής ψηφιακών πληροφοριών της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ (NSA)¹⁵. Προηγουμένως, ο όρος «μεταδεδομένα» αναφερόταν κυρίως σε στοιχεία, όπως τα αρχεία καταλόγου βιβλιοθηκών, τα λεξικά δεδομένων, και οι λέξεις-κλειδιά για ακαδημαϊκά άρθρα. Σήμερα φέρνει, επίσης, στο νου αρχεία καταγραφής κλήσεων κινητών τηλεφώνων, επικεφαλίδες ηλεκτρονικού ταχυδρομείου, ιστορικό αναζήτησης στο Διαδίκτυο, δεδομένα θέσης GPS¹⁶.

Τα μεταδεδομένα ορίζονται ως «δομημένη περιγραφή των βασικών χαρακτηριστικών ενός αντικειμένου και περιλαμβάνουν λεπτομέρειες, όπως το όνομα του συγγραφέα, την ημερομηνία δημοσίευσης, τη μορφή και το μέγεθος του αρχείου. Αυτά τα χαρακτηριστικά βοηθούν, ως επί το πλείστον, στην αποτελεσματική οργάνωση και ανάκτηση πληροφοριών. Αξίζει να σημειωθεί, ότι η διάκριση μεταξύ δεδομένων και μεταδεδομένων εξαρτάται συχνά από το πλαίσιο μέσα στο οποίο αυτά χρησιμοποιούνται. Αυτό που χαρακτηρίζεται ως «μεταδεδομένα» σε ένα σενάριο μπορεί να είναι πρωτογενή δεδομένα σε ένα άλλο, υπογραμμίζοντας τον πολύπλευρο ρόλο τους στη διαχείριση και επεξεργασία ενός συνόλου πληροφοριών¹⁷.

¹⁴ (Παπαδόπουλος, 2008)

¹⁵ (Landau, 2020), Διαθέσιμο σε: <https://dl.acm.org/doi/abs/10.1145/3442167.3442171>

¹⁶ (Mayernik, Acker, 2018), Διαθέσιμο σε: <https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.23927>

¹⁷ (Landau, 2020)

Τα μεταδεδομένα είναι πληροφορίες που παρέχουν μια δομημένη περιγραφή άλλων δεδομένων, βοηθώντας στην ταξινόμηση και τον προσδιορισμό των χαρακτηριστικών τους. Τα δεδομένα αυτά μπορούν να παραχθούν χειροκίνητα ή αυτόματα και συνήθως αποθηκεύονται σε μια εξειδικευμένη βάση δεδομένων. Παραδείγματα μεταδεδομένων περιλαμβάνουν λεπτομέρειες σχετικά με τη συγγραφή, τη δημιουργία και τις ημερομηνίες τροποποίησης για διάφορους τύπους περιεχομένου, όπως έγγραφα, εικόνες, βίντεο, βάσεις δεδομένων, υπολογιστικά φύλλα και ιστοσελίδες. Επιπλέον, τα μεταδεδομένα μπορούν να περιλαμβάνουν τεχνικές προδιαγραφές, όπως μορφή και μέγεθος αρχείου, δικαιώματα χρήσης και δεδομένα γεωγραφικού εντοπισμού, ενισχύοντας τη χρησιμότητά τους στη διαχείριση, αναζήτηση και οργάνωση μεγάλων συνόλων δεδομένων σε διάφορες πλατφόρμες¹⁸.

Στις Ηνωμένες Πολιτείες, η έννοια των μεταδεδομένων επικοινωνίας περιγράφεται λεπτομερώς σε διάφορα επίσημα κείμενα. Ο νόμος του 1986 για το απόρρητο των ηλεκτρονικών επικοινωνιών (ECPA) παρέχει ένα πλαίσιο για την προστασία των ηλεκτρονικών επικοινωνιών και περιλαμβάνει διατάξεις για το χειρισμό των μεταδεδομένων. Ο εν λόγω νόμος διασφαλίζει ότι τα μεταδεδομένα που σχετίζονται με τις ηλεκτρονικές επικοινωνίες, όπως τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα τηλεφωνικά αρχεία, προστατεύονται βάσει συγκεκριμένων κατευθυντήριων γραμμών για την προστασία της ιδιωτικής ζωής¹⁹. Όσον αφορά στα τηλεφωνικά μεταδεδομένα η κυβέρνηση των ΗΠΑ επέκτεινε τον ορισμό των τηλεφωνικών μεταδεδομένων μετά τις αποκαλύψεις του Snowden, ώστε να περιλαμβάνει, ενδεικτικά, «λεπτομερείς πληροφορίες δρομολόγησης, όπως δεδομένα αναγνώρισης της κλήσης, δηλαδή, αριθμούς τηλεφώνου προέλευσης και διεθνή αριθμό ταυτότητας συνδρομητή κινητής τηλεφωνίας (IMSI), αριθμούς τηλεφωνικών καρτών, μαζί με τους χρόνους και τη διάρκεια των κλήσεων»²⁰.

¹⁸ Big Blue Data Academy, «Τι Είναι τα Μεταδεδομένα (Metadata): Σημασία, Τύποι & Χρήσεις», Big Blue Data Academy, 01 Δεκεμβρίου 2023, Διαθέσιμο σε: <https://bigblue.academy/gr/metadedomena>

¹⁹ Electronic Communications Privacy Act of 1986 (ECPA), Bureau of Justice Assistance, US Department of Justice, Διαθέσιμο σε: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#1-0>

²⁰ In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc., No. BR 13- 80 (FISC Apr. 25, 2013), Διαθέσιμο σε: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-059.pdf>

Τα μεταδεδωμένα επικοινωνίας στην Ευρωπαϊκή Ένωση εξετάζονται εκτενώς, μέσα από τα νομοθετικά κείμενα, ιδίως σε κανονισμούς που αφορούν την προστασία της ιδιωτικής ζωής και τις ηλεκτρονικές επικοινωνίες. Σύμφωνα με την πρόταση για τον «Κανονισμό για την προστασία της ιδιωτικής ζωής και τις ηλεκτρονικές επικοινωνίες» (Regulation on Privacy and Electronic Communications ή αλλιώς ePrivacy Regulation)²¹, τα μεταδεδωμένα επικοινωνίας περιλαμβάνουν πληροφορίες, όπως οι αριθμοί που καλούνται από τα υποκείμενα, οι ιστότοποι που επισκέπτονται, οι γεωγραφικές τοποθεσίες, καθώς και η ώρα, η ημερομηνία και η διάρκεια των επικοινωνιών. Αυτά τα μεταδεδωμένα θεωρούνται ιδιαίτερα ευαίσθητα, καθώς μπορούν να αποκαλύψουν λεπτομερείς προσωπικές πληροφορίες για την ιδιωτική ζωή των ατόμων, συμπεριλαμβανομένων των κοινωνικών σχέσεων, των συνηθειών και των ενδιαφερόντων. Προστατευτικές διατάξεις εντοπίζονται και στο κείμενο του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ)²².

Οι εν λόγω κανονισμοί επιβάλλουν στους παρόχους υπηρεσιών επικοινωνίας, να χειρίζονται τα μεταδεδωμένα με το ίδιο επίπεδο προστασίας με το περιεχόμενο των επικοινωνιών, αντιλαμβανόμενοι αυτά ως προσωπικά δεδομένα. Στόχος είναι να διασφαλιστεί η εμπιστευτικότητα των ηλεκτρονικών επικοινωνιών και να προστατευθεί αποτελεσματικά, το δικαίωμα στην «ιδιωτική ζωή» των ατόμων. Οι εν λόγω κανονισμοί καλύπτουν, επίσης, τα δικαιώματα των τελικών χρηστών να ελέγχουν τα δεδομένα επικοινωνίας τους, συμπεριλαμβανομένης της δυνατότητας να αποτρέπουν την παρουσίαση της αναγνώρισης της γραμμής κλήσης και της δυνατότητας να περιορίζουν τις μη ζητηθείσες επικοινωνίες για σκοπούς άμεσης εμπορικής προώθησης.

Στην πραγματικότητα, δεν υπάρχει σαφής διάκριση μεταξύ μεταδεδωμένων επικοινωνίας και περιεχομένου αυτής. Έχουν υποστηριχθεί πολλές θεωρίες σχετικά με το ασafές της

²¹ Proposal for a *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/003 COD, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

²² Regulation (EU) 2016/679 on Privacy and Electronic Communications (GDPR), Διαθέσιμο σε: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

διάκρισης αλλά εν τέλει ο διαχωρισμός πρέπει να βασιστεί στο εκάστοτε πλαίσιο, μέσα στο οποίο, διεξάγεται η επικοινωνία²³.

2.1 Κατηγορίες μεταδεδομένων

Τα μεταδεδομένα χωρίζονται σε κατηγορίες ανάλογα με την λειτουργία που επιτελούν και το τελικό αποτέλεσμα. Υπάρχουν τα «διαχειριστικά μεταδεδομένα», τα οποία επιτρέπουν στον διαχειριστή που έχει πρόσβαση σε αυτά, να θέσει ένα συγκεκριμένο πλαίσιο για την πρόσβαση στην πληροφορία και να δημιουργήσει-αλλοιώσει τα δικαιώματα των χρηστών. Στη συνέχεια, τα «περιγραφικά μεταδεδομένα» επιτελούν τον ρόλο της περιγραφής-κατανόησης του περιεχομένου συγκεκριμένων δεδομένων χορηγώντας σημαντικά στοιχεία, όπως τίτλους, λέξεις-κλειδιά, περιλήψεις κ.α. Τα «δομικά μεταδεδομένα» λειτουργούν επεξηγηματικά ως προς τον τρόπο οργάνωσης των δεδομένων και την αλληλεπίδραση κομματιών των δεδομένων μεταξύ τους. Τα «στατιστικά μεταδεδομένα» παρέχουν στοιχεία σχετικά με την «ποιότητα και την αξιοπιστία» των δεδομένων και τέλος υπάρχουν και τα «νομικά μεταδεδομένα» τα οποία παρέχουν πληροφορίες σχετικά με «τον συγγραφέα, τον κάτοχο πνευματικών δικαιωμάτων, τους όρους άδειας χρήσης και τους περιορισμούς χρήσης»²⁴.

Συγκεκριμένα στα μεταδεδομένα επικοινωνίας αυτά χωρίζονται στις εξής κατηγορίες:²⁵

1. Χρονικά Δεδομένα: Πληροφορίες σχετικά με την ώρα και την ημερομηνία της επικοινωνίας.
2. Δεδομένα Διάρκειας: Η διάρκεια της επικοινωνίας.
3. Δεδομένα Συμμετεχόντων: Λεπτομέρειες για τα άτομα που συμμετέχουν στην επικοινωνία, όπως αριθμοί τηλεφώνου, διευθύνσεις email ή ονόματα χρήστη.
4. Δεδομένα Τοποθεσίας: Γεωγραφικές πληροφορίες που δείχνουν πού ξεκίνησε ή λήφθηκε η επικοινωνία, συχνά συλλέγονται μέσω GPS.

²³ Σύμφωνα με τον Kerr Orrin σε άρθρο στη Washington Post με τίτλο "Websurfing and the Wiretap Act," Washington Post, στις 4 Ιουνίου 2015 «η γραμμή μεταξύ περιεχομένου και μεταδεδομένων δεν είναι αφηρημένη αλλά συναφής με το πλαίσιο της κάθε επικοινωνίας».

²⁴ (Big Blue Data Academy, 2023)

²⁵ (Chia, 2023), Διαθέσιμο σε: https://www.splunk.com/en_us/blog/learn/metadata-types.html

5. Δεδομένα Συσκευών: Πληροφορίες για τις συσκευές που χρησιμοποιήθηκαν για την έναρξη ή τη λήψη της επικοινωνίας, συμπεριλαμβανομένων των τύπων συσκευών, των λειτουργικών συστημάτων και των πληροφοριών δικτύου.
6. Μέθοδος Επικοινωνίας: Το μέσο ή η πλατφόρμα που χρησιμοποιείται για την επικοινωνία, όπως τηλεφωνικές κλήσεις, email, μηνύματα κειμένου ή πλατφόρμες κοινωνικών μέσων.
7. Δεδομένα Δικτύου: Λεπτομέρειες για το δίκτυο μέσω του οποίου γίνεται η επικοινωνία, συμπεριλαμβανομένων των διευθύνσεων IP και των παρόχων υπηρεσιών.
8. Αναγνωριστικά Μηνυμάτων: Μοναδικά αναγνωριστικά για κάθε επικοινωνιακό συμβάν, όπως αναγνωριστικά κλήσεων ή αναγνωριστικά μηνυμάτων email.
9. Πληροφορίες Δρομολόγησης: Δεδομένα πορείας που δείχνουν πώς η επικοινωνία μεταδόθηκε μέσω διαφόρων κόμβων και δικτύων.
10. Πληροφορίες Συνημμένων: Μεταδεδομένα για οποιαδήποτε αρχεία ή συνημμένα που αποστέλλονται κατά τη διάρκεια της επικοινωνίας, συμπεριλαμβανομένων των ονομάτων και των τύπων αρχείων.

Στα μεταδεδομένα επικοινωνίας, οι γενικοί τύποι, όπως αναφέρθηκαν παραπάνω εμφανίζονται ως εξής: τα χρονικά δεδομένα (ημερομηνία και ώρα) και τα δεδομένα συμμετεχόντων (αποστολέας και παραλήπτης), για παράδειγμα, λειτουργούν ως «περιγραφικά μεταδεδομένα», βοηθώντας στον εντοπισμό των επικοινωνιακών συμβάντων. Τα δεδομένα συσκευών και δικτύου χρησιμεύουν ως «διαχειριστικά μεταδεδομένα», διαχειριζόμενα τις τεχνικές λεπτομέρειες και την πρόσβαση. Τα δεδομένα συσκευών μπορεί να περιλαμβάνουν πληροφορίες για τον τύπο της συσκευής που χρησιμοποιήθηκε, όπως ένα smartphone ή ένας υπολογιστής, καθώς και το λειτουργικό σύστημα.

Τα δεδομένα δικτύου περιλαμβάνουν πληροφορίες, όπως, η διεύθυνση IP και ο πάροχος υπηρεσιών διαδικτύου, οι οποίες βοηθούν στη διαχείριση της ασφάλειας και της πρόσβασης. Οι πληροφορίες δρομολόγησης και τα δεδομένα συνημμένων αντιπροσωπεύουν τα «δομικά μεταδεδομένα», οργανώνοντας τη ροή και τη δομή των επικοινωνιακών γεγονότων συμβάλλοντας στην ανάλυση και στην αρχειοθέτηση των

επικοινωνιών. Οι πληροφορίες δρομολόγησης δείχνουν τη διαδρομή που ακολουθεί μια επικοινωνία μέσω διαφόρων κόμβων και δικτύων, όπως η διαδρομή ενός email μέσω διαφορετικών διακομιστών.

Συνολικά, αυτά τα διάφορα είδη μεταδεδομένων συνεργάζονται για να παράσχουν ένα ολοκληρωμένο πλαίσιο για την κατανόηση των επικοινωνιακών δραστηριοτήτων, χωρίς να αποκαλύπτεται το περιεχόμενο των επικοινωνιών.

2.2.Περιπτώσεις χρήσης των μεταδεδομένων της επικοινωνίας

2.2.1 Παρακολούθηση στο πλαίσιο της επιβολής του νόμου

Τα μεταδεδομένα επικοινωνίας στη σημερινή ψηφιακή εποχή διαδραματίζουν ολοένα και αυξανόμενο ρόλο στο πεδίο της επιβολής του νόμου, παρέχοντας τα βασικά εργαλεία για την παρακολούθηση και την ανάλυση των προτύπων επικοινωνίας, χωρίς να εμβαθύνουν στο πραγματικό περιεχόμενο. Αυτά τα μεταδεδομένα αξιοποιούνται για την ανίχνευση ύποπτων δραστηριοτήτων, τον εντοπισμό πιθανών απειλών και τη χαρτογράφηση περίπλοκων δικτύων επικοινωνίας. Για παράδειγμα, το πρόγραμμα PRISM της NSA²⁶, το

²⁶ Το πρόγραμμα PRISM ήταν ένα μυστικό πρόγραμμα παρακολούθησης που ξεκίνησε από την Υπηρεσία Εθνικής Ασφάλειας (NSA) των Ηνωμένων Πολιτειών. Αποκαλύφθηκε στο κοινό μέσω εγγράφων που διέρρευσαν από τον Έντουαρντ Σνόουντεν τον Ιούνιο του 2013. Το PRISM επέτρεπε στην NSA να συλλέγει και να αναλύει τις διαδικτυακές επικοινωνίες από διάφορες μεγάλες διαδικτυακές εταιρείες. Στο πλαίσιο του PRISM, η NSA φέρεται να είχε άμεση πρόσβαση στους διακομιστές διαφόρων τεχνολογικών κολοσσών, όπως οι Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube και Apple. Μέσω αυτού του προγράμματος, η NSA μπορούσε να συλλέξει ένα ευρύ φάσμα δεδομένων, συμπεριλαμβανομένων των ηλεκτρονικών μηνυμάτων, των συνομιλιών, των φωτογραφιών, των βίντεο και των εγγράφων, καθώς και των μεταδεδομένων που σχετίζονται με αυτές τις επικοινωνίες. Αυτό προκάλεσε ευρεία ανησυχία για την προστασία της ιδιωτικής ζωής και τις πολιτικές ελευθερίες, καθώς έθεσε ερωτήματα σχετικά με την έκταση της κυβερνητικής επιτήρησης και την πιθανή παραβίαση των δικαιωμάτων των ατόμων στην ιδιωτική ζωή.

Οι αποκαλύψεις σχετικά με το PRISM πυροδότησαν μια παγκόσμια συζήτηση σχετικά με τις κυβερνητικές πρακτικές παρακολούθησης, τα δικαιώματα προστασίας της ιδιωτικής ζωής και την ισορροπία μεταξύ εθνικής ασφάλειας και πολιτικών ελευθεριών. Προκάλεσαν εκκλήσεις για μεταρρύθμιση, αυξημένη διαφάνεια και μεγαλύτερη εποπτεία των δραστηριοτήτων των υπηρεσιών πληροφοριών. Σε απάντηση στη δημόσια κατακραυγή, ορισμένες εταιρείες τεχνολογίας άρχισαν να εφαρμόζουν ισχυρότερα μέτρα κρυπτογράφησης για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση, ενώ οι κυβερνήσεις σε όλο τον κόσμο αντιμετώπισαν πιέσεις να επανεξετάσουν και να αναθεωρήσουν τις πολιτικές τους για την παρακολούθηση.

οποίο αποκαλύφθηκε από τον Edward Snowden, κατέδειξε πώς τα μεταδεδομένα μπορούν να συλλέγονται και να αναλύονται συστηματικά για την αποκάλυψη και την παρακολούθηση απειλών για την ασφάλεια. Με την ενδελεχή εξέταση των χρόνων επικοινωνίας, των συχνοτήτων και των σχέσεων των συμμετεχόντων, το PRISM επέτρεψε τον εντοπισμό ασυνήθιστων μοτίβων δραστηριότητας και συνδέσεων μεταξύ υπόπτων.

Η χρήση των μεταδεδομένων επικοινωνίας για τον εντοπισμό ύποπτων δραστηριοτήτων περιλαμβάνει την ανάλυση χρονικών ανωμαλιών και ασυνήθιστων συχνοτήτων επαφών. Η αναγνώριση μοτίβων μέσω της ανάλυσης μεταδεδομένων επιτρέπει στις αρχές να εντοπίζουν οργανωμένες εγκληματικές δραστηριότητες ή πιθανές τρομοκρατικές συνωμοσίες παρατηρώντας τις σχέσεις και τις αλληλεπιδράσεις εντός των δικτύων επικοινωνίας.

Η εκτεταμένη χρήση μεταδεδομένων επικοινωνίας από τον κυβερνητικό και από τον ιδιωτικό τομέα έχει γίνει όλο και πιο διαδεδομένη στο πεδίο της συλλογής πληροφοριών και δεδομένων. Χαρακτηριστικό παράδειγμα αποτελεί, η αλλαγή της εστίασης της NSA από το περιεχόμενο στα μεταδεδομένα της επικοινωνίας. Αναλύοντας το παράδειγμα, παρατηρούμε, ότι στα τέλη της δεκαετίας του 1990, η NSA άρχισε να αντιμετωπίζει σημαντικές προκλήσεις, καθώς η κύρια αποστολή της, δηλαδή η υποκλοπή, αποκρυπτογράφηση και ανάλυση των επικοινωνιών, περιπλεκόταν ολοένα και περισσότερο από την ταχεία ανάπτυξη της ψηφιακής επικοινωνίας.

Η έλευση του Διαδικτύου επέφερε εκθετική αύξηση του όγκου, της ποικιλομορφίας και της ταχύτητας ανταλλαγής δεδομένων. Επιπλέον, η ευρεία υιοθέτηση προηγμένων τεχνολογιών κρυπτογράφησης εμπόδισε, περαιτέρω, την ικανότητα της NSA να έχει πρόσβαση και να κατανοεί το περιεχόμενο των υποκλαπέντων μηνυμάτων, καθιστώντας αναγκαία την αλλαγή των στρατηγικών και των δυνατοτήτων της, ώστε να συμβαδίζει με το εξελισσόμενο ψηφιακό τοπίο.

Η στροφή προς τη χρήση μεταδεδομένων επικοινωνιών στις Η.Π.Α, μεταμόρφωσε σημαντικά την εργασία των υπηρεσιών πληροφοριών, ιδίως στον αμερικανικό στρατό και την NSA. Μέχρι τα μέσα της δεκαετίας του 2000, η έμφαση μετακινήθηκε από την απλή υποκλοπή και αποκωδικοποίηση του περιεχομένου των μηνυμάτων στη χαρτογράφηση

των δικτύων επικοινωνίας. Τεχνικές, όπως, η χρήση μη επανδρωμένων αεροσκαφών (drones) για την παρακολούθηση των αλληλεπιδράσεων και τον εντοπισμό προτύπων επικοινωνίας έγιναν κεντρικό στοιχείο των επιχειρήσεων.²⁷

Η κατανόηση αυτών των δικτύων παρείχε συχνά μεγαλύτερη στρατηγική αξία από το ίδιο το περιεχόμενο των μηνυμάτων, ιδίως σε ζώνες πολεμικών συγκρούσεων. Όπως δήλωσε ο γενικός σύμβουλος της NSA Stewart Baker, «τα μεταδεδομένα σας λένε απολύτως τα πάντα για τη ζωή κάποιου. Αν έχετε αρκετά μεταδεδομένα, δεν χρειάζεστε πραγματικά περιεχόμενο»²⁸, ενώ ακούγοντας την δήλωση αυτή ο πρώην αρχηγός της NSA στρατηγός Michael Hayden, είχε δηλώσει το 2014, «That description... is absolutely correct. We kill people based on metadata»²⁹. Η προσέγγιση αυτή υιοθετήθηκε σε παγκόσμιο επίπεδο, με διάφορα έθνη να αναγνωρίζουν το στρατηγικό πλεονέκτημα της εστίασης στα μεταδεδομένα.

Η άνοδος των συσκευών του Διαδικτύου των Πραγμάτων (IoT) και άλλων νέων πηγών δεδομένων υπογράμμισε περαιτέρω τη σημασία των μεταδεδομένων. Οι συσκευές IoT παράγουν εκτεταμένα μεταδεδομένα που μπορούν να αποκαλύψουν περίπλοκες λεπτομέρειες σχετικά με την καθημερινή ρουτίνα και τις τοποθεσίες των ανθρώπων. Για παράδειγμα, τα μεταδεδομένα μπορούν να δείξουν πότε τα άτομα βρίσκονται στο σπίτι, να υποδείξουν την παρουσία προσώπων σε ευαίσθητες περιοχές ή να παρακολουθήσουν συγκεκριμένες δραστηριότητες εντός ενός σπιτιού, όπως η χρήση έξυπνων οικιακών συσκευών ή τα πρότυπα ύπνου. Αυτά τα μεταδεδομένα είναι συχνά τα πιο αποκαλυπτικά παρέχοντας συνεχείς πληροφορίες για τη συμπεριφορά του χρήστη και το περιβάλλον του.

Η μετάβαση από την παραδοσιακή τηλεφωνία στις επικοινωνίες μέσω IP και κινητές συσκευές έχει αυξήσει κατά πολύ τον όγκο των μεταδεδομένων. Ενώ τα αρχεία κλήσεων από τα παραδοσιακά τηλεφωνικά συστήματα είναι σχετικά απλά και περιέχουν βασικές πληροφορίες, όπως η διάρκεια της κλήσης και οι συμμετέχοντες, οι επικοινωνίες που βασίζονται σε IP παράγουν πολύ πιο λεπτομερή μεταδεδομένα.

²⁷ (Landau, 2020)

²⁸(Cole, 2014), Διαθέσιμο σε: https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/?fbclid=IwZXh0bgNhZW0CMTEAAR1sd6MkUstJy2yOCmIxJoxwCqlcg4Jji3KfrHfS7q0NpqpX2vRUXPlvAUg_aem_-uZIFKYFcGPrHoEsV5OXVA

²⁹ (Ferran, 2014), Διαθέσιμο σε: https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/?fbclid=IwZXh0bgNhZW0CMTEAAR06rtLPQ6dfy4RV472JOWIUGIMykbe8aNPAIVSRTA_o5fHWzy_moHOzdC8_aem_q8fz0OLAA5S0xWE5hKUtVQ

Μια και μόνο διαδικτυακή αλληλεπίδραση μπορεί να περιλαμβάνει πολυάριθμα σημεία δεδομένων, προσφέροντας βαθιές πληροφορίες για τη συμπεριφορά του χρήστη και τα πρότυπα αλληλεπίδρασης. Οι εξελίξεις στην ψηφιακή τεχνολογία και τη μηχανική μάθηση της τεχνητής νοημοσύνης έχουν διευκολύνει την αναζήτηση και την ανάλυση αυτών των μεταδεδομένων, αποκαλύπτοντας σύνθετα μοτίβα και συνδέσεις που ήταν προηγουμένως δύσκολο να εντοπιστούν. Η εξέλιξη αυτή αναδεικνύει μια σημαντική αλλαγή στις πρακτικές επιτήρησης, προκαλώντας νέες ανησυχίες για την προστασία της ιδιωτικής ζωής.

2.3. Ανάλυση των όρων «εξωτερικά στοιχεία της επικοινωνίας» και «μεταδεδομένα»

Ο όρος «εξωτερικά στοιχεία» της επικοινωνίας εντοπίζεται στην θεωρία ως μια έννοια που περιγράφει όλα τα στοιχεία εκείνα που δεν θεωρούνται «περιεχόμενο» της επικοινωνίας. Αντίστοιχη κωδικοποίηση σε διεθνή κείμενα είναι τα «δεδομένα κίνησης» (traffic data) και τα «δεδομένα θέσης» (location data). Σαν «εξωτερικά στοιχεία» χαρακτηρίζονται όλα αυτά τα οποία περιβάλλουν το μήνυμα, όπως η διάρκεια της επικοινωνίας, ο τόπος και ο χρόνος που αυτή έλαβε χώρα, η ταυτότητα των υποκειμένων που επικοινωνούν κ.α. Αναλυτικότερα, ως «δεδομένα κίνησης» χαρακτηρίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία, με σκοπό, τη διαβίβαση μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή τη χρέωση της επικοινωνίας αυτής και περιλαμβάνει δεδομένα σχετικά με τη δρομολόγηση, τη διάρκεια ή το χρόνο μιας επικοινωνίας, τους αριθμούς των καλουμένων και καλούντων³⁰ ενώ «δεδομένα θέσης» καλούνται τα δεδομένα που επεξεργάζονται από υπηρεσία ηλεκτρονικών επικοινωνιών και υποδεικνύουν τη θέση του τερματικού εξοπλισμού ενός χρήστη το υψόμετρο του τερματικού εξοπλισμού, την κατεύθυνση κίνησης του χρήστη και τον χρόνο καταγραφής των πληροφοριών θέσης³¹.

Σχετικά με την ορολογία των στοιχείων επικοινωνίας, έχουν προταθεί στην ελληνική θεωρία αρκετές διαφοροποιήσεις, με στόχο, να περιγραφεί καταλληλότερα ο σκοπός τους

³⁰ ICO, Διαθέσιμο σε: <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/communications-networks-and-services/traffic-data/#trafficdata>

³¹ ICO, Διαθέσιμο σε: <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/communications-networks-and-services/traffic-data/#trafficdata>

σε σχέση με το περιεχόμενο της επικοινωνίας, καθώς και η αλληλεπίδρασή τους με αυτό³². Στη σύγχρονη ορολογία έχει υιοθετηθεί και ο όρος μεταδεδομένα επικοινωνίας, όπως περιγράφηκε και ανωτέρω. Στην ελληνική θεωρία χρησιμοποιούνται και οι δύο όροι με ισοδύναμο τρόπο, ενώ, η ελληνική νομολογία δεν έχει υιοθετήσει τον σύγχρονο όρο μεταδεδομένα και αναφέρεται αποκλειστικά σε «εξωτερικά στοιχεία» της επικοινωνίας ως αντιδιαστολή στο περιεχόμενο αυτής. Η σημασία αυτής της διάκρισης είναι πρωτίστως σημειολογική, καθώς πίσω από κάθε όρο κρύβεται διαφορετική νομική μεταχείριση, όπως θα εξηγηθεί κατωτέρω.

Κομβικό ζήτημα στην ελληνική έννομη τάξη αποτελεί το αν τα «εξωτερικά στοιχεία» της επικοινωνίας ή τα μεταδεδομένα υπάγονται στην συνταγματική προστασία του άρθρου 19 παρ.1 εδ. α' του Συντάγματος και κατ' επέκταση αν εντάσσονται στις εγγυητικές διατάξεις των εκτελεστικών νόμων σχετικά με την άρση του απορρήτου των επικοινωνιών. Το ΕΔΔΑ έχει κρίνει στην υπόθεση Malone κατά Ηνωμένου Βασιλείου, πως τα «εξωτερικά στοιχεία» της επικοινωνίας υπάγονται στο προστατευτέο πεδίο του άρθρου 8 της ΕΣΔΑ και ως εκ τούτου ενδεχόμενη απόκτησή τους θα πρέπει να ακολουθεί τους θεσμοθετημένους τρόπους με τις ανάλογες δικαστικές και νομικές εγγυήσεις.

3. Η κατοχύρωση του δικαιώματος του απορρήτου της επικοινωνίας σε διεθνές επίπεδο

Στο πλαίσιο της παγκόσμιας συνδεσιμότητας, η καθιέρωση του δικαιώματος στο απόρρητο της επικοινωνίας σε διεθνές επίπεδο, αποτελεί κομβική στιγμή στην νομική ιστορία. Το θεμελιώδες αυτό δικαίωμα, αποτελεί τον ακρογωνιαίο λίθο πάνω στον οποίο ευδοκίμει η ανταλλαγή ιδεών, πληροφοριών και πολιτισμού πέρα από τα σύνορα. Ειδικά μετά τον Β' Παγκόσμιο Πόλεμο η «οικουμενικότητα» των ανθρωπίνων δικαιωμάτων αποτελεί σημαντική κατάκτηση του ανθρωπίνου πολιτισμού. Το κεφάλαιο αυτό εξετάζει την εξέλιξη και τις σύγχρονες προκλήσεις που περιβάλλουν την καθιέρωση του δικαιώματος στην επικοινωνία σε παγκόσμια κλίμακα.

³² Βλ. Ν. Λίβος: Η προστασία των συνδετικών δεδομένων των τηλεπικοινωνιών, ΠοινΧρ 1997 (ΜΖ') σελ. 747 επ.

3.1 Διεθνή κείμενα

Στο άρθρο 12 της Οικουμενικής Διακήρυξης Δικαιωμάτων του Ανθρώπου, η προστασία του απορρήτου της επικοινωνίας εδράζεται στην προστασία της «ιδιωτικής σφαίρας» και ο προστατευτικός πυρήνας αυτής έγκειται στην προστασία από «αυθαίρετες» επεμβάσεις στην «ιδιωτικότητα» των μερών. Το συγκεκριμένο άρθρο, όπως και το αντίστοιχο άρθρο του ελληνικού Συντάγματος, επιδέχεται περιορισμών, οι οποίοι επιβάλλονται με το άρθρο 29 παρ.2 της ΟικΔιακΔΑ. Οι εν λόγω περιορισμοί είναι αυτοί που καθιερώνει ο ίδιος ο νόμος, προς χάρη των δικαιωμάτων και των ελευθεριών των άλλων και για να ικανοποιούνται οι δίκαιες απαιτήσεις της ηθικής και της δημόσιας τάξης και της γενικής ευημερίας σε μια δημοκρατική κοινωνία³³.

Στο ίδιο πρότυπο και στο ίδιο πνεύμα κατοχυρώνεται στο άρθρο 17 του Διεθνούς Συμφώνου Ατομικών και Πολιτικών Δικαιωμάτων, η προστασία της «ιδιωτικότητας», με περιεχόμενο την προστασία του απορρήτου της επικοινωνίας δια του αποκλεισμού των «αυθαίρετων ή παράνομων παρενοχλήσεων. Το εύρος της προστασίας εκτείνεται στην θετική προστασία του δικαιώματος εκ μέρους του Κράτους, παίρνοντας τα κατάλληλα μέτρα (όπως νομοθετικά) και στην αρνητική αξίωση των φυσικών προσώπων να απέχει το Κράτος από κάθε προσβολή του εν λόγω δικαιώματος. Στο εν λόγω άρθρο δεν προβλέπονται νομοθετικοί περιορισμοί στο δικαίωμα.

Η προστασία του απορρήτου των επικοινωνιών εντοπίζεται και στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ), όπου ακολουθώντας την λογική της ΟικΔιακΔΑ, προστατεύει εν συνόλω το δικαίωμα στην ιδιωτική ζωή του ατόμου, συμπεριλαμβανομένου και του απορρήτου της επικοινωνίας.

3.2 Άρθρο 8 ΕΣΔΑ

Το άρθρο 8 ΕΣΔΑ προστατεύει την υπό ευρεία έννοια «ιδιωτική-απόρρητη σφαίρα» του ατόμου, η οποία αναλύεται σε επιμέρους εκφάνσεις-δικαιώματα. Πρώτον το δικαίωμα στο σεβασμό της ιδιωτικής ζωής του, δεύτερον στον σεβασμό της οικογενειακής ζωής του, τρίτον στον σεβασμό της κατοικίας του και τέλος στον σεβασμό της αλληλογραφίας του.

³³ (Παπαδόπουλος, 2008)

Τα επιμέρους δικαιώματα αυτά τελούν σε σχέση επικάλυψης, δηλαδή μπορούν να παραβιαστούν ένα και περισσότερα με μία μόνο πράξη ή παράλειψη³⁴.

Καθώς ο σεβασμός στην αλληλογραφία είναι αμυντικό ατομικό δικαίωμα, προστατεύονται οι φορείς του δικαιώματος αυτού, ήτοι φυσικά και νομικά πρόσωπα, από την χωρίς δικαίωμα επέμβαση του Κράτους στο δικαίωμα αυτό, είτε μέσω της αποχής της παρέμβασης στην άσκηση του δικαιώματος είτε μέσω της δημιουργίας συνθηκών κατάλληλων για την απόλαυση του δικαιώματος. Η αποχή από την παρέμβαση στο δικαίωμα επιδέχεται συγκεκριμένων μόνο περιορισμών, οι οποίοι εντοπίζονται στην δεύτερη παράγραφο του άρθρου, για τους οποίους θα γίνει λόγος κατωτέρω.

Κατά την προσπάθεια ερμηνείας του άρθρου 8 ΕΣΔΑ, οφείλει κάποιος να ανατρέξει στην νομολογία του ΕΔΔΑ. Το πεδίο εφαρμογής του άρθρου 8, παράλληλα με την έκταση της προστασίας που παρέχει, περιλαμβάνει και τα κριτήρια για τους επιτρεπόμενους περιορισμούς τα οποία καθορίζονται, μέσω της νομολογίας του Δικαστηρίου. Η πλούσια νομολογία του ΕΔΔΑ περιλαμβάνει ερμηνείες σχετικά με το τι συνιστά ιδιωτική και οικογενειακή ζωή, καθώς και τις προϋποθέσεις υπό τις οποίες τα δικαιώματα αυτά μπορούν να περιοριστούν νομίμως, παρέχοντας ένα πλαίσιο για την κατανόηση της περίπλοκης ισορροπίας μεταξύ των ατομικών ελευθεριών και των κοινωνικών συμφερόντων.

Είναι σημαντικό να αναφερθεί πως το ΕΔΔΑ έχει προχωρήσει σε διασταλτική ερμηνεία στην προστατευόμενη έννοια του απορρήτου της αλληλογραφίας υπό το άρθρο 8, μέσα στο οποίο έχει εντάξει τα εξωτερικά στοιχεία της επικοινωνίας ³⁵ (όπως οι εισερχόμενες-εξερχόμενες κλήσεις, γεωγραφική θέση του χρήστη)³⁶ τα οποία, μάλιστα, θεωρούνται «αναπόσπαστο στοιχείο της τηλεφωνικής επικοινωνίας»³⁷. Στα εξωτερικά στοιχεία περιλαμβάνει και αναλυτικούς λογαριασμούς τηλεφωνικών επικοινωνιών που αναγράφουν στοιχεία όπως ημερομηνία, χρόνος, διάρκεια και κόστος κλήσεων.

³⁴ (Τσόλιας, 2021)

³⁵ (Αλεξοπούλου, 2017)

³⁶ *Malone v. the United Kingdom*

³⁷ (Τσόλιας, 2021)

3.3 Περιορισμοί του άρθρου 8 ΕΣΔΑ

Οι περιορισμοί του άρθρου 8 προβλέπονται στη δεύτερη παράγραφο αυτού, αλλά, εφαρμόζονται υπό συγκεκριμένα κριτήρια. Πρώτον, πρέπει να προβλέπεται σε νόμο του Κράτους, οι λόγοι περιορισμού του δικαιώματος να αναφέρονται στο νόμο και ο εν λόγω περιορισμός να τηρεί την αρχή της αναλογικότητας υπό ευρεία έννοια σύμφωνα με τις αρχές μιας δημοκρατικής κοινωνίας³⁸.

Οι περιορισμοί που θέτει το ΕΔΔΑ στο εν λόγω άρθρο παρατίθενται εξαντλητικά και ερμηνεύονται πάντα στενά και υπό το πρίσμα της εξαίρεσης από τον κανόνα του απόλυτα απαραβίαστου του ατομικού δικαιώματος της προστασίας της αλληλογραφίας.

Ο πρώτος επιτρεπτός περιορισμός του δικαιώματος, που τίθεται στην δεύτερη παράγραφο του άρθρου 8, είναι οι περιπτώσεις που συντρέχουν λόγοι εθνικής ασφάλειας, όπου αυτό και με βάση την πάγια νομολογία του ΕΔΔΑ, κρίνεται στη βάση συγκεκριμένων εκτιμήσεων και δεν απαιτείται μια εξαντλητική και περιοριστική απαρίθμηση στην εκάστοτε εθνική νομοθεσία.

Ο δεύτερος επιτρεπτός περιορισμός αφορά την διακρίβωση εγκλημάτων, όπως αναφέρονται στην εθνική νομοθεσία με μόνο απαραίτητο ερμηνευτικό εργαλείο την περιγραφή της φύσεως των εγκλημάτων αυτών. Για το νόμιμο της επέμβασης αυτής στο δικαίωμα, το ΕΔΔΑ έχει αναπτύξει στην νομολογία του³⁹ τις απαραίτητες εγγυήσεις που πρέπει να τηρούνται, ανάμεσα στις οποίες είναι να υπάρχουν «σοβαρές ενδείξεις ενοχής» και με τη σειρά τους να συνοδεύονται από μια «σοβαρή αιτιολογία»⁴⁰.

4. Κατοχύρωση της προστασίας του απορρήτου της επικοινωνίας σε Ευρωπαϊκό επίπεδο

Η κατοχύρωση της προστασίας του απορρήτου της επικοινωνίας εντάσσεται στην προστασία της ιδιωτικής και οικογενειακής ζωής, η οποία στην έννομη τάξη της ΕΕ προστατεύεται περαιτέρω ως θεμελιώδες ανθρώπινο δικαίωμα. Τα θεμελιώδη δικαιώματα,

³⁸ (Τσόλιας, 2021)

³⁹ Βλ. *Iordachi and Others v. Moldova*, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%22itemid%22:%22001-91245%22>

⁴⁰ (Αλεξοπούλου, 2017, σελ. 473)

αποτελούν γενικές αρχές δικαίου στην ενωσιακή έννομη τάξη και δεσμεύουν όλα τα όργανά της και δεν μπορεί να υπάρξει αντίθετη πρόβλεψη σε ενωσιακό κανόνα δικαίου.

Η προστασία γενικώς των θεμελιωδών ανθρωπίνων δικαιωμάτων διαπερνάει το σύνολο των κανόνων δικαίου τόσο του πρωτογενούς δικαίου της Ένωσης, του παράγωγου όσο και της νομολογίας του ΔΕΕ και του ΕΔΔΑ. Στην Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ) και συγκεκριμένα στην παράγραφο 1 του άρθρου 6 ρητά αναφέρεται η προστασία των θεμελιωδών δικαιωμάτων, ενώ στην παράγραφο 2 του ίδιου άρθρου κατοχυρώνεται η προστασία τους με βάση την Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ).

Όπως αναφέρθηκε ανωτέρω, η προστασία του απορρήτου των επικοινωνιών προστατεύεται ως ειδικότερη έκφανση του σεβασμού της ιδιωτικής ζωής στο άρθρο 8 της ΕΣΔΑ, στο οποίο γίνεται ρητή αναφορά στη ΣΕΕ. Όταν υιοθετήθηκε ο Χάρτης των Θεμελιωδών Δικαιωμάτων, στο άρθρο 7 κατοχυρώθηκε η προστασία της ιδιωτικής και οικογενειακής ζωής, με τρόπο αντίστοιχο αυτού του άρθρου 8 της ΕΣΔΑ. Ο ΧΘΔ μετά την υπογραφή της Συνθήκης της Λισαβόνας μετατρέπεται σε πρωτογενές ευρωπαϊκό δίκαιο και έχει την ίδια ισχύ με τις Συνθήκες της Ένωσης, ενώ, τότε πραγματοποιήθηκε και η προσχώρηση της ΕΕ στην ΕΣΔΑ.

4.1. Παράγωγο δίκαιο της ΕΕ

Πριν προχωρήσουμε στην ανάλυση του παράγωγου δικαίου που αποτελεί σήμερα το ισχύον νομοθετικό πλαίσιο, σχετικά με τα μεταδεδομένα επικοινωνίας, αξίζει να σημειωθούν κάποια ζητήματα. Με την ισχύουσα ευρωπαϊκή νομοθεσία τα μεταδεδομένα της επικοινωνίας θεωρούνται προσωπικά δεδομένα και η νομική αντιμετώπισή τους τόσο σε ζητήματα επεξεργασίας τους, διατήρησής τους αλλά και επέμβασης στον απόρρητο χαρακτήρα αυτών ως έκφανση του δικαιώματος στην ιδιωτική ζωή, διέπεται από τον νομικό αυτό χαρακτηρισμό. Αποτελεί, δε, πλέον και πάγια νομολογία του ΕΔΔΑ και του ΔΕΕ, όπως θα αναλυθεί και στη συνέχεια. Όμως δεν ήταν πάντα ένα τόσο ξεκάθαρο ζήτημα και πολλές απόψεις στην θεωρία αλλά και στη νομολογία, δεν θεωρούσαν ότι τα μεταδεδομένα επικοινωνίας ήταν δεδομένα που οδηγούσαν στην ταυτότητα του υποκειμένου των μεταδεδομένων.

4.2 Οδηγία 2002/58/EK (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες -E Privacy Directive)

Πρόκειται για την Οδηγία⁴¹ που αντικατέστησε την κατηρημένη Οδηγία 97/66/EK, η οποία προσπάθησε να αντιμετωπίσει πολλά ζητήματα, επεκτείνοντας το πεδίο εφαρμογής της, ώστε να καλύπτει ένα ευρύτερο φάσμα ηλεκτρονικών επικοινωνιών και επικαιροποιώντας τις διατάξεις, ώστε να αντικατοπτρίζουν καλύτερα τις τεχνολογικές εξελίξεις και τους ρυθμούς της αγοράς στις αρχές της δεκαετίας του 2000. Η Οδηγία αυτή αποτελεί εξειδίκευση της Οδηγίας 95/46/EK για την προστασία των δεδομένων προσωπικού χαρακτήρα και μάλιστα έχει τροποποιηθεί δύο φορές, η μια με την Οδηγία 2006/24/EK, σχετικά με το ζήτημα της διατήρησης των δεδομένων και η δεύτερη με την ψήφιση της Οδηγίας 2009/136/EK.

Η Οδηγία διεύρυνε το πεδίο εφαρμογής, το οποίο πλέον καταλάμβανε όλες τις ηλεκτρονικές επικοινωνίες και εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όσον αφορά στην παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών εντός της ΕΕ.

Για πρώτη φορά στην Οδηγία εισάγεται ο όρος «δεδομένα θέσης», και αναφέρονται ως «δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και υποδεικνύουν την θέση του τερματικού εξοπλισμού του χρήστη της υπηρεσίας». Σχετικά με τα δεδομένα κίνησης, ορίζεται στο άρθρο 6, ότι πρέπει να διαγράφονται ή να καθίστανται ανώνυμα όταν δεν χρειάζονται πλέον για τον σκοπό της μετάδοσης μιας επικοινωνίας.

Αντίθετα η νόμιμη χρήση και επεξεργασία των «δεδομένων θέσης», έγκειται στην συγκατάθεση του χρήστη ή στην ανωνυμοποίηση αυτών, ενώ, οι χρήστες πρέπει και να ενημερώνονται για την επεξεργασία των δεδομένων αυτών. Η Οδηγία θέσπισε για πρώτη φορά την απαίτηση για συγκατάθεση μετά από ενημέρωση πριν από την αποθήκευση ή την πρόσβαση σε πληροφορίες στη συσκευή ενός χρήστη, γνωστή ως «νόμος για τα

⁴¹ Οδηγία 2002/58/EK, Διαθέσιμη σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058>

cookies», καθώς ρητά εισήγαγε στο προστατευτικό πεδίο του απορρήτου τα δεδομένα που περιλαμβάνονταν στα cookies, κάτι που μέχρι τότε αμφισβητούνταν έντονα.

Παρ' όλα αυτά οι διατάξεις της Οδηγίας για τα δεδομένα κίνησης είναι ασαφείς, ιδίως όσον αφορά τη διατήρηση των δεδομένων και δεν προσφέρουν απόλυτη προστασία. Η Οδηγία απαιτεί τη διαγραφή ή την ανωνυμοποίηση των δεδομένων κίνησης, όταν δεν χρειάζονται πλέον για τη μετάδοση ή την τιμολόγηση, αλλά επιτρέπει εξαιρέσεις για σκοπούς όπως οι πληρωμές διασύνδεσης και η πρόληψη της απάτης. Ταυτοχρόνως, αν και η Οδηγία επιτρέπει την επεξεργασία «δεδομένων θέσης», με τη συγκατάθεση του χρήστη ή αν τα δεδομένα είναι ανώνυμα, οι ευρείες εξαιρέσεις για υπηρεσίες έκτακτης ανάγκης και υπηρεσίες προστιθέμενης αξίας θεωρούνται υπερβολικά επεκτατικές και ανεπαρκώς καθορισμένες, με κίνδυνο κατάχρησης της επεξεργασίας δεδομένων θέσης.

Η εφαρμογή των διατάξεων της Οδηγίας είναι ασυνεπής, με τις εθνικές ρυθμιστικές αρχές να διαφέρουν ως προς τους πόρους και τη δέσμευση, με αποτέλεσμα να υπάρχουν διαφορετικά επίπεδα προστασίας σε ολόκληρη την ΕΕ. Η ραγδαία εξέλιξη τεχνολογιών όπως τα smartphones και οι υπηρεσίες που βασίζονται στην τοποθεσία έχει ξεπεράσει την Οδηγία, αφήνοντας κενά στην προστασία των χρηστών. Τα ζητήματα αυτά υπογράμμισαν την ανάγκη για ένα πιο ολοκληρωμένο και προσαρμόσιμο ρυθμιστικό πλαίσιο, οδηγώντας στην ανάπτυξη ενός νέου κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με στόχο την παροχή ισχυρότερης, σαφέστερης και συνεκτικότερης προστασίας της ιδιωτικής ζωής σε ευθυγράμμιση με τον ΓΚΠΔ.

4.3 Η Οδηγία 2006/24/EK (Data Retention Directive)

Η Οδηγία 2006/24/EK, γνωστή ως Οδηγία για τη διατήρηση δεδομένων⁴², ήταν εξειδίκευση της Οδηγίας 2002/58/EK, για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με στόχο την καταπολέμηση του σοβαρού εγκλήματος, συμπεριλαμβανομένης της τρομοκρατίας, μέσω της διατήρησης τηλεπικοινωνιακών δεδομένων. Η Οδηγία αντανακλά το κλίμα της εποχής, όπου η Ευρώπη έχει βιώσει μια

⁴² Η διατήρηση δεδομένων περιλαμβάνει τη συλλογή μεταδεδομένων κίνησης και θέσης χωρίς να απαιτείται αρχικά υποψία εγκληματικής δραστηριότητας ή δικαστική εποπτεία, με σκοπό τη μετέπειτα χρήση τους από την επιβολή του νόμου. Η διαδικασία αυτή διαφέρει από την υποκλοπή του περιεχομένου της επικοινωνίας (υποκλοπή) ή τη φύλαξη δεδομένων, όπου οι αρχές ζητούν ειδικά από τους φορείς εκμετάλλευσης να διατηρήσουν τα δεδομένα συγκεκριμένων ατόμων που είναι ύποπτα για εγκληματική δραστηριότητα.

σειρά τρομοκρατικών επιθέσεων⁴³ και η νομοθεσία των οργάνων αλλά και η νομολογία της ΕΕ, θεώρησε πως η γενική διατήρηση μεταδεδομένων επικοινωνίας θα αποτελούσε ένα ισχυρό όπλο απέναντι στον πόλεμο κατά της τρομοκρατίας.

Η Οδηγία απαιτούσε από τους παρόχους τηλεπικοινωνιακών και διαδικτυακών υπηρεσιών να διατηρούν «δεδομένα κίνησης» και «θέσης» για χρονικά διαστήματα που κυμαίνονταν από έξι μήνες έως δύο έτη, ώστε να είναι διαθέσιμα στις εθνικές αρχές για λόγους εθνικής και δημόσιας ασφάλειας και για την πρόληψη, την διακρίβωση και την καταστολή σοβαρών ποινικών αδικημάτων, ανεξάρτητα από τη συμμετοχή τους σε οποιαδήποτε εγκληματική δραστηριότητα, το οποίο ήταν ένα δυσανάλογο μέτρο που παραβίαζε τα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και την προστασία του απορρήτου των δεδομένων. Χαρακτηριστικό είναι, μάλιστα, το γεγονός πως η υποχρέωση διατήρησης εκ μέρους των παρόχων αφορούσε μόνο τα μεταδεδομένα της επικοινωνίας και όχι το περιεχόμενο.

Το σημείο καμπής ήρθε το 2014, όταν το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) κήρυξε την Οδηγία 2006/24/ΕΚ ανίσχυρη. Το δικαστήριο διαπίστωσε ότι η οδηγία παρενέβαινε δυσανάλογα στα θεμελιώδη δικαιώματα της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα, καθώς δεν καθόριζε σαφείς και ακριβείς κανόνες σχετικά με την έκταση της παρέμβασης. Μετά την απόφαση του ΔΕΕ, η Οδηγία έπαψε να έχει ισχύ, αφήνοντας τα κράτη μέλη να αντιμετωπίσουν το νομικό κενό. Ορισμένες χώρες κατήργησαν τους νόμους τους για τη διατήρηση δεδομένων, ενώ άλλες προσπάθησαν να καταρτίσουν νέα νομοθεσία που να συμμορφώνεται με τις αρχές του ΔΕΕ, τονίζοντας την ανάγκη για αναλογικά, αναγκαία και σεβόμενα τα θεμελιώδη δικαιώματα μέτρα.

Η Οδηγία 2006/24/ΕΚ, ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 3917/2011. Ο νόμος αυτός εισήγαγε υποχρέωση διατήρησης των μεταδεδομένων για ένα έτος για τα εγκλήματα που αναφέρονται στον σχετικό νόμο, δηλαδή στον ισχύοντα σήμερα ν. 5002/2022. Ωστόσο, όταν η απόφαση *Digital Rights Ireland* του ΔΕΕ το 2014 έκρινε την Οδηγία ως μη σύμφωνη με την αρχή της αναλογικότητας, λόγω της γενικευμένης και αδιάκριτης φύσης της διατήρησης δεδομένων, η Ελλάδα δεν πήρε καμία πρωτοβουλία να εναρμονίσει την νομοθεσία της με το ενωσιακό δίκαιο, με αποτέλεσμα ο ν. 3917/2011 να είναι ακόμη και σήμερα σε ισχύ. Επομένως, εξακολουθεί να προβλέπει την υποχρέωση διατήρησης

⁴³ Τρομοκρατικές επιθέσεις στη Νέα Υόρκη το 2001, στην Μαδρίτη το 2004 και στο Λονδίνο το 2005

δεδομένων κίνησης και θέσης από τους παρόχους για ένα έτος, με σκοπό την καταπολέμηση σοβαρών εγκλημάτων, όπως αυτά ορίζονται στο άρθρο 4 του νόμου και συνδέονται με τα αδικήματα του ν. 5002/2022. Παρά το ότι το ΔΕΕ και σε μεταγενέστερες αποφάσεις του, όπως στις υποθέσεις *Tele2 Sverige AB* και *Watson*, κατέστησε σαφές ότι η διατήρηση δεδομένων επιτρέπεται μόνο υπό αυστηρές προϋποθέσεις, όπως η ύπαρξη συγκεκριμένων, σοβαρών απειλών για την εθνική ασφάλεια, η περιορισμένη χρονική διάρκεια και η επαρκής προστασία από κατάχρηση, στην Ελλάδα η έλλειψη επικαιροποίησης του εθνικού πλαισίου προς εναρμόνιση με τις ενωσιακές απαιτήσεις και τις επιταγές της νομολογίας ΕΔΔΑ και του ΔΕΕ εξακολουθεί να αποτελεί ανοιχτό ζήτημα.

4.4 Πρόταση για τον Κανονισμό e-Privacy

Η πρόταση για τον Κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, που έχει σχεδιαστεί για να αντικαταστήσει την οδηγία του 2002 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, σηματοδοτεί μια σημαντική αλλαγή στο τοπίο της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες στην Ευρωπαϊκή Ένωση. Ο εν λόγω κανονισμός επιδιώκει να ευθυγραμμιστεί με τα αυστηρά πρότυπα προστασίας δεδομένων που θέτει ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ).

Η πρόταση Κανονισμού θέτει αυστηρούς κανόνες για την επεξεργασία των μεταδεδομένων και ορίζει τις προϋποθέσεις υπό τις οποίες οι πάροχοι υπηρεσιών μπορούν να έχουν πρόσβαση στα δεδομένα που είναι αποθηκευμένα στις συσκευές των χρηστών. Μια αξιοσημείωτη απαίτηση είναι, ότι οποιαδήποτε πρόσβαση ή χρήση τέτοιων δεδομένων πρέπει να βασίζεται στη συγκατάθεση του χρήστη, αντανακλώντας τα αυξημένα πρότυπα προστασίας της ιδιωτικής ζωής του ΓΚΠΔ. Στόχο αποτελεί ο εξορθολογισμός της διαδικασίας της επαναλαμβανόμενης συναίνεσης και η εκ των προτέρων δυνατότητα ρύθμισης της συγκατάθεσης ή μη στις ρυθμίσεις του προγράμματος περιήγησης, με την συμβολή των παρόχων των αντίστοιχων υπηρεσιών.

Σχετικά με την διατήρηση των δεδομένων, που είναι και ένα σημαντικό ζήτημα που διαφοροποιεί την πρόταση του Κανονισμού από την κατηρηγμένη Οδηγία 2006/24/EK, προβλέπεται πως το περιεχόμενο των ηλεκτρονικών επικοινωνιών διαγράφεται όταν δεν είναι πλέον απαραίτητο για το σκοπό της επεξεργασίας, ενώ τα μεταδεδομένα διαγράφονται ή καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για την παροχή

των αντίστοιχων υπηρεσιών. Η διάταξη αυτή δέχεται βάσιμη κριτική λόγω του εύρους της σημασίας του αντικτύπου της. Συγκεκριμένα, η διατήρηση των δεδομένων θα πρέπει να προβλέπεται αυστηρά και με συγκεκριμένα χρονικά όρια για να θεωρείται σύννομη και όχι να προβλέπεται σε γενικού τύπου διατάξεις.

Παρά τις θετικές αλλαγές, οι επιμέρους διατάξεις για την επεξεργασία των δεδομένων ηλεκτρονικών επικοινωνιών, οι διατάξεις για τα Cookies κι εν γένει της αποθήκευσης και επεξεργασίας των πληροφοριών που βρίσκονται στον τερματικό εξοπλισμό των τελικών χρηστών δημιουργούν ανασφάλεια δικαίου, εξαιτίας των διευρυσμένων εξαιρέσεων από τον γενικό κανόνα απαγόρευσης και των γενικόλογων αναφορών σε αυτές. Εξίσου ανασφάλεια, προκαλεί η διάταξη για την διατήρηση των δεδομένων ηλεκτρονικών επικοινωνιών, εξαιτίας της έλλειψης σαφών ορίων και προβλέψεων. Δεν θα πρέπει σύμφωνα και με την Επιτροπή EDPS (European Data Protection Supervisor), η διεύρυνση του πεδίου εφαρμογής του Κανονισμού και στα μεταδεδομένα, να ερμηνευτεί ως γενική εντολή επέκτασης των καθεστώτων διατήρησης δεδομένων από τα κράτη-μέλη⁴⁴.

4.5 Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ-GDPR)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018, αντιπροσωπεύει μια ουσιαστική αναθεώρηση του πλαισίου προστασίας δεδομένων της Ευρωπαϊκής Ένωσης, αντικαθιστώντας την Οδηγία για την Προστασία Δεδομένων του 1995 (Οδηγία 95/46/EK). Ο ΓΚΠΔ κατηγοριοποιεί τα μεταδεδομένα κίνησης και θέσης ως δεδομένα προσωπικού χαρακτήρα όταν μπορούν να συνδεθούν με ένα αναγνωρίσιμο άτομο. Αυτή η ταξινόμηση εισαγάγει τα δεδομένα αυτά στις αυστηρές προστατευτικές δικλίδες και απαιτήσεις του ΓΚΠΔ.

⁴⁴ (EDPS, 2017), Opinion 6/2017, Διαθέσιμη σε: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

5. Νομολογιακή Επισκόπηση σε Ευρωπαϊκό επίπεδο

5.1 Αποφάσεις ΕΔΔΑ

5.1.1 Malone κατά Ηνωμένου Βασιλείου

Τον Αύγουστο του 1984, το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ) εξέδωσε απόφαση στην υπόθεση Malone κατά Ηνωμένου Βασιλείου⁴⁵. Το ΕΔΔΑ εξέτασε δύο δραστηριότητες για πιθανές παραβιάσεις του άρθρου 8 ΕΣΔΑ: την υποκλοπή τηλεφωνικών συνομιλιών και τη δημοσιοποίηση πληροφοριών που αποκτήθηκαν μέσω «τηλεφωνικής μέτρησης» (metering). Κεντρική έμφαση δόθηκε στον χειρισμό των δεδομένων θέσης και κίνησης, ιδίως μέσω της πρακτικής της «μέτρησης»⁴⁶. Η μέτρηση αφορά τη συστηματική καταγραφή των τηλεφωνικών αριθμών που καλούνται, μαζί με μεταδεδομένα όπως η διάρκεια και ο χρόνος της κλήσης. Επρόκειτο, λοιπόν, για την συγκέντρωση των μεταδεδομένων επικοινωνίας.

Το βασικό ζήτημα για το ΕΔΔΑ ήταν κατά πόσον οι παρεμβάσεις αυτές δικαιολογούνταν βάσει του άρθρου 8 παρ. 2, καθώς ήταν «σύμφωνες με τον νόμο» και «αναγκαίες σε μια δημοκρατική κοινωνία». Το Δικαστήριο τόνισε ότι το «σύμφωνα με το νόμο» απαιτούσε όχι μόνο τη συμμόρφωση με το εθνικό δίκαιο αλλά και την ποιότητα του δικαίου αυτού (ο νόμος πρέπει να είναι προσιτός και προβλέψιμος).

Το Ηνωμένο Βασίλειο υποστήριξε ότι αυτές οι απαιτήσεις ήταν λιγότερο σημαντικές σε υποθέσεις μυστικής παρακολούθησης, αλλά το Δικαστήριο διαφώνησε, υποστηρίζοντας ότι οι μυστικές δραστηριότητες απαιτούσαν ακόμη μεγαλύτερη νομική προστασία από την αυθαίρετη χρήση και την παράνομη επέμβαση. Ο ίδιος ο νόμος έπρεπε να ορίζει με σαφήνεια το πεδίο εφαρμογής και τον τρόπο διακριτικής ευχέρειας για την υποκλοπή επικοινωνιών, ώστε να προστατεύονται τα άτομα από αυθαίρετες παρεμβάσεις.

Το Δικαστήριο διαπίστωσε ότι το αγγλικό δίκαιο σχετικά με την υποκλοπή επικοινωνιών ήταν «ασαφές και ανοικτό σε διαφορετικές ερμηνείες», στερούμενο «εύλογης βεβαιότητας

⁴⁵ Malone v. The United Kingdom, Διαθέσιμο σε: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57532%22%7D>

⁴⁶ (Schade, 1985) Διαθέσιμο σε: https://www.jstor.org/stable/4506727?read-now=1&seq=3#page_scan_tab_contents

σχετικά με το ποια στοιχεία των εξουσιών υποκλοπής διέπονται από νομικούς κανόνες και τι παρέμενε στη διακριτική ευχέρεια της εκτελεστικής εξουσίας»⁴⁷.

5.1.2 Roman Zakharov κατά Ρωσίας

Στην υπόθεση ορόσημο Zakharov κατά Ρωσίας⁴⁸ (4 Δεκεμβρίου 2015), το ΕΔΔΑ εξέτασε το ρωσικό νομικό πλαίσιο που διέπει την παρακολούθηση των επικοινωνιών κινητής τηλεφωνίας. Ο προσφεύγων, Roman Zakharov, δημοσιογράφος, υποστήριξε ότι οι νόμοι επέτρεπαν τη μαζική παρακολούθηση χωρίς επαρκείς εγγυήσεις, παραβιάζοντας το δικαίωμά του στην ιδιωτική ζωή σύμφωνα με το άρθρο 8 και το δικαίωμά του σε αποτελεσματική προσφυγή σύμφωνα με το άρθρο 13 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ).

Το Δικαστήριο υπογράμμισε τον κίνδυνο ότι ένα μυστικό σύστημα μαζικής παρακολούθησης θα μπορούσε να χρησιμοποιηθεί καταχρηστικά για την υπονόμευση ή ακόμη και την καταστροφή της δημοκρατίας υπό το πρόσχημα της προστασίας της. Κατά την εξέταση, το Δικαστήριο κατέληξε στο συμπέρασμα, ότι το ρωσικό νομικό πλαίσιο για την παρακολούθηση των επικοινωνιών δεν διέθετε επαρκείς εγγυήσεις κατά της αυθαίρετης χρήσης και κατάχρησης του συστήματος.

Στην απόφαση Zakharov, το Δικαστήριο υποστήριξε με αποφασιστικότητα ότι δεν πρέπει να επιτρέπεται η μαζική συλλογή μεγάλου όγκου δεδομένων. Το Δικαστήριο υπογράμμισε το θεμελιώδες ζήτημα, πως η απουσία των απαραίτητων μηχανισμών αδειοδότησης και εποπτείας καθιστούσε αδύνατο να διαπιστωθεί εάν είχαν σημειωθεί παραβιάσεις της ιδιωτικής ζωής.

Το ΕΔΔΑ αξιολόγησε τις αρχές που απαιτούνται για να προσδιοριστεί αν η επέμβαση ήταν «αναγκαία σε μια δημοκρατική κοινωνία». Υπογράμμισε την εγγενή ένταση μεταξύ των μέτρων που θεσπίζονται για λόγους ασφαλείας και των επιπτώσεών τους στην κοινωνία την οποία αποσκοπούν να προστατεύσουν και την αναγκαιότητα ισχυρών και αποτελεσματικών εγγυήσεων κατά της κατάχρησης. Η δικαστική εξουσιοδότηση, σημείωσε, είναι ανεπαρκής εάν συνεπάγεται απλώς επιφανειακή εμπλοκή. Αντιθέτως, οι δικαστές πρέπει να έχουν επαρκή εξουσιοδότηση, επομένως και αιτιολογία, για να

⁴⁷ (Schade, 1985)

⁴⁸ Roman Zakharov v. Russia, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-159324%22%7D>

διαπιστώνουν την ύπαρξη εύλογων υποψιών κατά ενός ατόμου. Επιπλέον, το δικαστικό σώμα πρέπει να διαθέτει την εξουσία να αξιολογεί την αναλογικότητα και την αναγκαιότητα των μέτρων παρακολούθησης.

Η υπόθεση Zakharov αποτελεί βασική εγγύηση για τα δικαιώματα των ευρωπαϊκών πολιτών. Επιβεβαιώνει ότι τα άτομα έχουν το δικαίωμα να υπερασπίζονται τα δικαιώματά τους όταν θεωρούν ότι αυτά παραβιάζονται από το κράτος, και επιβάλλει ότι το κράτος πρέπει πάντα να παρέχει μηχανισμό για την υποβολή τέτοιων καταγγελιών. Επιπλέον, η σημασία της υπόθεσης Zakharov υπερβαίνει την υπεράσπιση του άρθρου 8, καθώς το Δικαστήριο έχει αποδείξει την προθυμία του να εξετάσει και να αμφισβητήσει την εγκυρότητα ολόκληρων συστημάτων παρακολούθησης⁴⁹.

5.1.3 Szabó και Vissy κατά Ουγγαρίας

Η τελική απόφαση⁵⁰ δημοσιεύτηκε στις 06 Ιουνίου 2016 και αφορούσε την νομιμότητα των πρακτικών παρακολούθησης της Ουγγαρίας, όπως αποτυπώνονταν στην αντιτρομοκρατική νομοθεσία του 2011, η οποία παρείχε στις Εθνικές Υπηρεσίες Ασφαλείας εκτεταμένες εξουσίες για τη διεξαγωγή μυστικών επιχειρήσεων παρακολούθησης⁵¹.

Το ΕΔΔΑ διαπίστωσε, ότι η νομοθεσία ενέκρινε εκτεταμένα και παρεμβατικά μέτρα παρακολούθησης, όπως η κρυφή καταγραφή συνομιλιών, η υποκλοπή επιστολών και δεμάτων και η παρακολούθηση ηλεκτρονικών επικοινωνιών και ότι η διαδικασία εξουσιοδότησης εξαρτιόταν αποκλειστικά από τη διακριτική εξουσία έγκρισης των κυβερνητικών οργάνων, χωρίς επαρκή δικαστικό έλεγχο ή εγγυήσεις. Το Δικαστήριο κατέληξε στο συμπέρασμα, ότι ο ευρύς και αδιάκριτος χαρακτήρας αυτών των πρακτικών παρακολούθησης δεν ήταν ούτε αναγκαίος ούτε αναλογικός σε μια δημοκρατική κοινωνία, παραβιάζοντας έτσι το άρθρο 8 της ΕΣΔΑ.

Σημειώνεται ότι οι εξουσιοδοτούντες φορείς απέτυχαν να διενεργήσουν αξιολογήσεις της απόλυτης αναγκαιότητας και το κρίσιμο είναι ότι δεν υπήρχε δικαστική εποπτεία των δραστηριοτήτων επιτήρησης. Αν και η προστασία της εθνικής ασφάλειας αποτελούσε

⁴⁹ (De Hert, Bocos, 2015), Διαθέσιμο σε: <https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/>

⁵⁰ Szabó and Vissy v. Hungary, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-16002%22%5D%7D>

⁵¹(Privacy International), Ανακτήθηκε από: <https://privacyinternational.org/legal-action/szabo-v-hungary-hungary-mass-surveillance>

νόμιμο στόχο για τη θέσπιση και εφαρμογή μέτρων επιτήρησης, το Δικαστήριο τόνισε ότι οι ελάχιστες εγγυήσεις ήταν απαραίτητες για να διασφαλιστεί επαρκής και αποτελεσματική προστασία από την κατάχρηση.

Ελλείπει τέτοιων εγγυήσεων, τα μέτρα επιτήρησης ήταν δυσανάλογα, καθώς προωθούσαν την αντίληψη της απεριόριστης εκτελεστικής εξουσίας που επεμβαίνει στην ιδιωτική ζωή των πολιτών αντικαθιστώντας, έτσι, την τρομοκρατική απειλή με την απειλή της υπερβολής της εκτελεστικής εξουσίας.

Το ΕΔΔΑ στην απόφασή του αυτή όχι μόνο αμφισβήτησε τη συμβατότητά ενός εθνικού συστήματος μαζικής παρακολούθησης σε σχέση με τα δικαιώματα της Σύμβασης, αλλά και έθεσε μια αυστηρή απαίτηση για την ύπαρξη «ατομικών υποψιών» σε βάρος ενός πολίτη προτού επιτραπεί η παρακολούθηση, δίνοντας μάλιστα έμφαση στο γεγονός πως η κυβέρνηση δεν είχε αποδείξει την πρακτική αποτελεσματικότητα οποιωνδήποτε ρυθμίσεων εποπτείας⁵².

Πρόκειται για την υιοθέτηση μιας πολύ πιο αυστηρής στάσης σε σχέση με την εγχώρια παρακολούθηση, όπως είχε κάνει και στην υπόθεση Zakharov. Στην Szabó και Vissy το ΕΔΔΑ περιόρισε το κριτήριο του «αναγκαίου σε μια δημοκρατική κοινωνία», όσον αφορά στην μαζική παρακολούθηση για λόγους που εμπίπτουν στο άρθρο 8 παρ.2 ΕΣΔΑ, εξειδικεύοντας το σε αυτό της «απόλυτης αναγκαιότητας». «Ένα μέτρο μυστικής παρακολούθησης μπορεί να κριθεί ότι είναι σύμφωνο με τη Σύμβαση μόνο εάν είναι απολύτως αναγκαίο, ως γενική σκέψη, για τη διαφύλαξη των δημοκρατικών θεσμών και, επιπλέον, εάν είναι αυστηρά αναγκαίο, ως ειδικότερο κριτήριο, για την απόκτηση ζωτικής σημασίας πληροφοριών σε μια μεμονωμένη επιχείρηση»⁵³.

Σύμφωνα με αυτό το κριτήριο, θα έπρεπε οι αρχές να υποχρεούνται να εξετάζουν τις προϋποθέσεις για την υποκλοπή των επικοινωνιών κατά περίπτωση, ενώ ταυτοχρόνως η απαίτηση ότι τα μέτρα μυστικής παρακολούθησης πρέπει να είναι απολύτως αναγκαία για τη συλλογή «ζωτικής σημασίας» πληροφοριών σε μια συγκεκριμένη επιχείρηση είχε την λογική να καταστήσει πιθανότατα ασύμβατες με το άρθρο 8 τις συνήθεις επιχειρήσεις των

⁵² (Watt, 2021) Ανακτήθηκε από: <https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/>

⁵³ Szabó και Vissy κατά Ουγγαρίας (2016), παρ. 73

αρχών επιτήρησης, με αποτέλεσμα να είναι πρακτικά αδύνατο να τηρηθούν σε περιπτώσεις αλγοριθμικής επιτήρησης⁵⁴.

Παρ' όλα αυτά δεν είναι υπεράνω κριτικής η απόφαση αυτή, καθώς υπαναχώρησε από την Zakharov και στην σκέψη 71 το ΕΔΔΑ επέλεξε το χαμηλότερο κριτήριο της ανεπιφύλακτης «ατομικής υποψίας», το οποίο μειώνει σημαντικά τον βαθμό προστασίας που καθορίστηκε στην υπόθεση Roman Zakharov και προηγουμένως στην υπόθεση Iordachi το οποίο καθιέρωνε το κριτήριο της «εύλογης υποψίας». Όπως σημειώνει και ο δικαστής Pinto de Albuquerque⁵⁵ «ο πραγματικός λόγος για τον οποίο το σκεπτικό του Τμήματος δεν παραμένει πιστό στο κριτήριο της «εύλογης υποψίας» του Τμήματος μείζονος συνθέσεως- στην Zakharov- είναι επειδή υποθέτει ότι η καταπολέμηση της τρομοκρατίας απαιτεί μια «δεξαμενή πληροφοριών που μπορούν να ανακτηθούν από τις αρχές που εφαρμόζουν εξαιρετικά αποτελεσματικές μεθόδους και επεξεργάζονται μάζες δεδομένων, ενδεχομένως για κάθε πρόσωπο, εάν αυτό, με τον ένα ή τον άλλο τρόπο, συνδέεται με ύποπτα υποκείμενα ή αντικείμενα σχεδιαζόμενων τρομοκρατικών επιθέσεων»[35]. Η αοριστία αυτής της γλώσσας είναι εντυπωσιακή, καθώς συμπυκνώνει το διευρυνόμενο στο δίκτυο, καθολικό, μινιμαλιστικό όριο υποψίας που υποτίθεται ότι απαιτείται για την αποτελεσματική καταπολέμηση της τρομοκρατίας.

Επιπλέον, μια τέτοια αισιόδοξη γλώσσα είναι ενδεικτική μιας απατηλής πεποίθησης ότι η παγκόσμια επιτήρηση είναι ο *deus ex machina* που μπορεί να καταπολεμήσει τη μάστιγα της παγκόσμιας τρομοκρατίας. Ακόμη χειρότερα, μια τέτοια απατηλή γλώσσα εξαφανίζει το γεγονός ότι η υαλοποίηση της κοινωνίας φέρνει μαζί της τον οργουελιανό εφιάλτη του 1984. Στην πράξη, το Επιμελητήριο επιδοκιμάζει, για να χρησιμοποιήσουμε τα λόγια του Ευρωπαϊκού Κοινοβουλίου, "την εγκαθίδρυση ενός πλήρους προληπτικού κράτους, αλλάζοντας το καθιερωμένο παράδειγμα του ποινικού δικαίου στις δημοκρατικές κοινωνίες, σύμφωνα με το οποίο κάθε επέμβαση στα θεμελιώδη δικαιώματα των υπόπτων πρέπει να εγκρίνεται από δικαστή ή εισαγγελέα βάσει εύλογης υποψίας και να ρυθμίζεται από το νόμο, προωθώντας αντ' αυτού ένα μείγμα δραστηριοτήτων επιβολής του νόμου και πληροφοριών με θολές και αποδυναμωμένες νομικές εγγυήσεις, συχνά μη σύμφωνες με τους δημοκρατικούς

⁵⁴ (Kosta, 2017), Διαθέσιμο σε: <https://library.oapen.org/bitstream/id/e85a3ae4-6696-4449-9f39-51cd2e4d1953/SSRN-id3167723.pdf>

⁵⁵ Concurring [opinion](#) of judge Pinto de Albuquerque

ελέγχους και τις ισορροπίες και τα θεμελιώδη δικαιώματα, ιδίως το τεκμήριο αθωότητας"[37]».

5.1.4 Centrum för Rättvisa κατά Σουηδίας

Η υπόθεση Centrum för Rättvisa⁵⁶ έλαβε χώρα το 2008 εν μέσω δημόσιου διαλόγου στη Σουηδία σχετικά με την έκδοση του σουηδικού νόμου, για τις υπηρεσίες πληροφοριών σημάτων και των συναφών καταστατικών (συλλογικά γνωστών ως «νόμος FRA»). Κατά συνέπεια, η Σουηδία είχε το δικό της εγχώριο ισοδύναμο των αποκαλύψεων του Σνόουντεν και της επακόλουθης δημόσιας συζήτησης το 2007-2008.⁵⁷ Στις 19 Ιουνίου 2018, ένα τμήμα του ΕΔΔΑ κατέληξε ομόφωνα στο συμπέρασμα ότι δεν υπήρξε παραβίαση του άρθρου 8 της Σύμβασης.

Μετά από παραπομπή, η υπόθεση εξετάστηκε από το τμήμα μείζονος συνθέσεως, το οποίο εξέδωσε την απόφασή του στις 25 Μαΐου 2021, υπογραμμίζοντας διάφορες σημαντικές πτυχές. Το τμήμα μείζονος συνθέσεως ασχολήθηκε, από κοινού, με τα κριτήρια του ΕΔΔΑ «σύμφωνα με το νόμο» και «αναγκαιότητα», ανανεώνοντας τα παλιότερα κριτήρια από τις υποθέσεις Weber και Saravia και Liberty. Στο πλαίσιο της μαζικής υποκλοπής και διατήρησης μεταδεδομένων επικοινωνίας, το τμήμα μείζονος συνθέσεως δήλωσε ότι τα δεδομένα αυτά θα πρέπει να υπόκεινται στις ίδιες εγγυήσεις με το περιεχόμενο. Το τμήμα μείζονος συνθέσεως έκρινε ότι η Σουηδία παραβίασε το άρθρο 8 για τρεις λόγους: α) την έλλειψη σαφούς κανόνα για την καταστροφή του υποκλαπέντος υλικού χωρίς προσωπικά δεδομένα β) την απουσία πρόβλεψης στον νόμο, σχετικά με την λήψη κατάλληλων εγγυήσεων όσον αφορά το δικαίωμα στην ιδιωτική ζωή κατά την ανταλλαγή πληροφοριών με ξένους εταίρους και γ) την έλλειψη αποτελεσματικού εκ των υστέρων ελέγχου.

Αυτό που παρέλειψε να εξετάσει το Δικαστήριο, όμως είναι την πραγματική χρήση του σουηδικού νόμου και τις πρακτικές των μυστικών υπηρεσιών της Σουηδίας, γιατί η ύπαρξη νομικών κανόνων και θεσμών δεν διασφαλίζει πάντα ότι οι επιβλαβείς πρακτικές περιορίζονται - ο νόμος μπορεί επίσης να διευκολύνει τις πρακτικές αυτές⁵⁸. Αυτή η

⁵⁶ Centrum för Rättvisa v. Sweden, Διαθέσιμο σε: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-210078%22%5D%7D>

⁵⁷ (Klamberg, 2021) Διαθέσιμο σε: https://verfassungsblog.de/raettvisa/?fbclid=IwZXh0bgNhZW0CMTEAAR3WZY1AdP8G1fSkJlpf4VI9MhOYA_1vBd9J6LjdY9CNBAjh8dUKx4TpQk_aem_yq-juiSiChN_mUTobogtBg

⁵⁸ (Klamberg, 2021)

έλλειψη αυστηρού ελέγχου θα μπορούσε να οφείλεται σε διάφορους παράγοντες, όπως η πιθανή έλλειψη τεχνολογικής εμπειρογνωμοσύνης ή η πεποίθηση ότι η εθνική ασφάλεια είναι κατά βάση αρμοδιότητα της εκτελεστικής εξουσίας και όχι της δικαστικής εξουσίας. Αυτό εγείρει το ερώτημα κατά πόσον τα δικαστήρια, τόσο τα εθνικά όσο και τα διεθνή, θα μπορούσαν ποτέ να επιβλέψουν αποτελεσματικά την κρατική παρακολούθηση που διεξάγεται για σκοπούς εθνικής ασφάλειας.

5.1.5 Big Brothers Watch and Others κατά Ηνωμένου Βασιλείου

Η υπόθεση Big Brother Watch⁵⁹ και άλλοι κατά Ηνωμένου Βασιλείου είναι μια υπόθεση ορόσημο που εξέτασε σημαντικές ανησυχίες σχετικά με τη μαζική παρακολούθηση και τις επιπτώσεις της στα δικαιώματα ιδιωτικής ζωής βάσει της ΕΣΔΑ, κυρίως σε σχέση με τα προγράμματα μαζικής παρακολούθησης που αφορούσαν τη μαζική υποκλοπή επικοινωνιών, την ανταλλαγή πληροφοριών με ξένες κυβερνήσεις και την απόκτηση δεδομένων επικοινωνιών από παρόχους υπηρεσιών. Οι προσφεύγοντες υποστήριξαν ότι οι εν λόγω πρακτικές παρακολούθησης παραβίαζαν τα άρθρα 8 (δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής) και 10 (ελευθερία έκφρασης) της ΕΣΔΑ.

Στην απόφασή του τον Σεπτέμβριο του 2018, το Δικαστήριο αναγνώρισε ότι, ενώ τα καθεστώτα μαζικής υποκλοπής δεν παραβιάζουν εγγενώς τη Σύμβαση, το καθεστώς του Ηνωμένου Βασιλείου δεν διέθετε τις απαραίτητες εγγυήσεις, ιδίως όσον αφορά την επιλογή και την εξέταση του υποκλαπέντος υλικού παραβιάζοντας, έτσι, ευθέως το άρθρο 8. Περαιτέρω, όσον αφορά την απόκτηση δεδομένων επικοινωνιών από παρόχους υπηρεσιών, ειδικά όσον αφορά τους δημοσιογράφους, δεν διέθετε επαρκή εποπτεία, παραβιάζοντας έτσι τα άρθρα 8 και 10.

Μία από τις σημαντικότερες επισημάνσεις του ΕΔΔΑ ήταν, ότι η πρόσβαση σε μεταδεδομένα επικοινωνίας μπορεί να είναι εξίσου παρεμβατική με την πρόσβαση στο περιεχόμενο των επικοινωνιών, συνεχίζοντας την πάγια νομολογιακή πρακτική της ένταξης των μεταδεδομένων επικοινωνίας στον προστατευτέο πυρήνα του δικαιώματος της ιδιωτικής ζωής, μέσα στο οποίο εντάσσεται και το απόρρητο των επικοινωνιών.⁶⁰

⁵⁹ Big Brother Watch and others v. UK, Διαθέσιμο σε:

<https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>

⁶⁰ (Christakis, 2018), Διαθέσιμο σε: <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch->

Στην υπόθεση Big Brother Watch, το Δικαστήριο υπογράμμισε περαιτέρω ότι «η μαζική υποκλοπή αποτελεί πολύτιμο μέσο για την επίτευξη των επιδιωκόμενων νόμιμων σκοπών, ιδίως δεδομένου του σημερινού επιπέδου απειλής τόσο από την παγκόσμια τρομοκρατία όσο και από το σοβαρό έγκλημα»⁶¹.

Το σημαντικό στοιχείο που άρχισε να διαφαίνεται, είναι πως το επίκεντρο έχει μετατοπιστεί από την αμφισβήτηση της νομιμότητας των πολιτικών μαζικής παρακολούθησης στην αντιμετώπιση του τρόπου με τον οποίο θα πρέπει να εφαρμόζονται σωστά. Αυτό που καθρεφτίζει η απόφαση του ΕΔΔΑ είναι η νέα «κανονικότητα» στην Ευρώπη, η οποία περιλαμβάνει την αυξανόμενη επικράτηση των νόμων περί πληροφοριών που ενσωματώνουν το στοιχείο της «μαζικής παρακολούθησης».

Εκτός από τον έντονο κοινωνικοπολιτικό χαρακτήρα που έχει αυτή η διαπίστωση, αξίζει να σημειωθεί πως η αποδοχή της μαζικής παρακολούθησης από το ΕΔΔΑ αντιβαίνει στην νομολογία της ΕΕ και συγκεκριμένα στις αποφάσεις του ΔΕΕ. Για το ΔΕΕ ο αδιάκριτος και ευρύς χαρακτήρας της μαζικής συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ακόμη και με σκοπό την προστασία των ατόμων από σοβαρά εγκλήματα, εγκυμονεί σημαντικούς κινδύνους για τα ανθρώπινα δικαιώματα και τις ατομικές ελευθερίες.

Στην απόφαση «Digital Rights Ireland (2014)» το ΔΕΕ σημείωνε, πως «οι παρεκκλίσεις και οι περιορισμοί σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα πρέπει να εφαρμόζονται μόνο στο μέτρο που είναι απολύτως αναγκαίο». Στην απόφασή «Schrems» του 2015, το ΔΕΕ δήλωσε σαφώς ότι «η νομοθεσία που επιτρέπει στις δημόσιες αρχές να έχουν πρόσβαση σε γενικευμένη βάση στο περιεχόμενο των ηλεκτρονικών επικοινωνιών πρέπει να θεωρηθεί ότι θέτει σε κίνδυνο την ουσία του θεμελιώδους δικαιώματος σεβασμού της ιδιωτικής ζωής, όπως κατοχυρώνεται από το άρθρο 7 του Χάρτη». Στο ίδιο πνεύμα⁶² και η «Ομάδα εργασίας του άρθρου 29»⁶³, δημοσίευσε μία έκθεση Δεκέμβριο του 2018, στην οποία επανέλαβε την πάγια θέση της ότι «η μαζική και αδιάκριτη

[judgment/?fbclid=IwZXh0bgNhZW0CMTEAAR1E0V_rGxMyiJaS5SeOIUmu1gI-INrHWsmUv4bxjE_O2yKxbzE3gZ3ZQWw_aem_mCMs2-HN040O3PvVfdSbXg](https://eur-lex.europa.eu/judgment/?fbclid=IwZXh0bgNhZW0CMTEAAR1E0V_rGxMyiJaS5SeOIUmu1gI-INrHWsmUv4bxjE_O2yKxbzE3gZ3ZQWw_aem_mCMs2-HN040O3PvVfdSbXg)

⁶¹ (Christakis, 2018)

⁶² (Christakis, 2018)

⁶³ γνωστή πλέον ως Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων από τότε που τέθηκε σε ισχύ ο ΓΚΠΔ

παρακολούθηση ατόμων δεν μπορεί ποτέ να θεωρηθεί αναλογική και απολύτως αναγκαία σε μια δημοκρατική κοινωνία, όπως απαιτείται στο πλαίσιο της προστασίας που προσφέρουν τα ισχύοντα θεμελιώδη δικαιώματα»⁶⁴.

5.1.6. Οι αποφάσεις του τμήματος Μείζονος Συνθέσεως για την υπόθεση Big Brother Watch κατά του Ηνωμένου Βασιλείου και Centrum för Rättvisa κατά Σουηδίας

Στις 25 Μαΐου 2021 το ΕΔΔΑ εξέδωσε την απόφαση του Τμήματος Μείζονος Σύνθεσης για υπόθεση Big Brother Watch κατά του Ηνωμένου Βασιλείου και για την υπόθεση Centrum för Rättvisa κατά Σουηδίας, σχετικά με τα καθεστώτα μαζικής παρακολούθησης. Το τμήμα μείζονος συνθέσεως σ' αυτές τις αποφάσεις αναγνωρίζει, ότι η νομολογία του σχετικά με τη μαζική υποκλοπή χρειάζεται περαιτέρω ανάπτυξη. Τάσσεται υπέρ των «εγγυήσεων από άκρη σε άκρη», προτείνοντας, ότι σε εθνικό επίπεδο, κάθε στάδιο της διαδικασίας θα πρέπει να αξιολογείται ως προς την αναγκαιότητα και την αναλογικότητα. Επιπλέον, η μαζική υποκλοπή θα πρέπει να απαιτεί ανεξάρτητη έγκριση από την αρχή, όταν καθορίζονται οι στόχοι και το πεδίο εφαρμογής της επιχείρησης και η επιχείρηση θα πρέπει να υπόκειται σε εποπτεία και ανεξάρτητη επανεξέταση εκ των υστέρων.

Επιπλέον δημιουργεί ένα νέο σύνολο οκτώ κριτηρίων για το νόμιμο της παρακολούθησης από τις μυστικές υπηρεσίες πληροφοριών. Τα κριτήρια αυτά έχουν ως εξής: α) τους λόγους για τους οποίους μπορεί να επιτραπεί η μαζική υποκλοπή β) τις περιστάσεις υπό τις οποίες μπορεί να υποκλαπούν οι επικοινωνίες ενός ατόμου γ) τη διαδικασία που πρέπει να ακολουθείται για τη χορήγηση της άδειας δ) τις διαδικασίες που πρέπει να ακολουθούνται για την επιλογή την εξέταση και τη χρήση του υλικού της υποκλοπής ε) τις προφυλάξεις που πρέπει να λαμβάνονται κατά την κοινοποίηση του υλικού σε άλλα μέρη στ) τα όρια της διάρκειας της υποκλοπής, της αποθήκευσης του υλικού υποκλοπής και τις περιστάσεις υπό τις οποίες το υλικό αυτό πρέπει να διαγράφεται και να καταστρέφεται ζ) τις διαδικασίες και τους τρόπους εποπτείας από ανεξάρτητη αρχή της συμμόρφωσης με τις ανωτέρω εγγυήσεις και τις εξουσίες της για την αντιμετώπιση της μη συμμόρφωσης η) τις διαδικασίες για τον ανεξάρτητο εκ των υστέρων έλεγχο της εν λόγω συμμόρφωσης και τις

⁶⁴ (Article 29 Data Protection Working Party, 2017), Διαθέσιμο σε: http://ec.europa.eu/justice/data-protection/index_en.htm

εξουσίες που ανατίθενται στον αρμόδιο φορέα για την αντιμετώπιση περιπτώσεων μη συμμόρφωσης⁶⁵.

Παρό' όλα αυτά το ΕΔΔΑ φαίνεται να υπαναχωρεί σταδιακά από τη στάση του παρελθόντος όσον αφορά τη μαζική παρακολούθηση, αποδεχόμενο όλο και περισσότερο τα καθεστώτα μαζικής παρακολούθησης που εφαρμόζουν οι εθνικές υπηρεσίες πληροφοριών. Αυτή η μετατόπιση μπορεί να θεωρηθεί ως «πισωγύρισμα» για το ΕΔΔΑ, το οποίο μειώνει τις απαιτήσεις του για να διευκολύνει τις κρατικές πρακτικές, κανονικοποιώντας έτσι τη μαζική παρακολούθηση. Η εξέλιξη αυτή είναι ιδιαίτερα ανησυχητική, ειδικά αν εξετασθεί συνδυαστικά με το αντίστοιχο «πισωγύρισμα» του ΔΕΕ στην υπόθεση *La Quadrature du Net and others*. Νομιμοποιώντας αυτά τα εκτεταμένα μέτρα παρακολούθησης, το ΕΔΔΑ κινδυνεύει να υπονομεύσει την προστασία των ατομικών δικαιωμάτων ιδιωτικής ζωής που κατοχυρώνονται στην ΕΣΔΑ. Αυτή η τάση προς την κανονικοποίηση της μαζικής παρακολούθησης εγείρει κρίσιμα ερωτήματα σχετικά με κατά πόσον τα δικαστήρια παραιτούνται από το ρόλο τους ως ελέγχου της εκτελεστικής εξουσίας, όταν η συζήτηση οδηγείται στο πεδίο της επιτήρησης.

5.1.7 Benedik κατά Σλοβενίας

Στην υπόθεση Benedik κατά Σλοβενίας⁶⁶ το Τέταρτο Τμήμα του Δικαστηρίου, στη απόφαση που δημοσιεύτηκε τις 24 Απριλίου 2018, έκρινε ότι η σλοβενική αστυνομία παραβίασε το άρθρο 8 και συγκεκριμένα το κριτήριο της συμφωνίας με τον νόμο⁶⁷. Η παραβίαση συνίσταται στην πρόσβαση της αστυνομίας σε πληροφορίες συνδρομητών που συνδέονταν με μια «δυναμική διεύθυνση IP», χωρίς πρώτα να λάβει δικαστικό ένταλμα⁶⁸.

⁶⁵ (Vogiatzoglou, 2018), Διαθέσιμο σε: <https://strasbourgobservers.com/2018/07/09/bulk-interception-of-communications-in-sweden-meets-convention-standards-the-latest-addition-to-mass-surveillance-case-law-by-the-european-court-of-human-rights/>

⁶⁶Υπόθεση Benedik κατά Σλοβενίας: <https://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22benedik%22%2C%22documentcollectionid%22:%5B%22GRANDCHAMBER%22%2C%22CHAMBER%22%2C%22itemid%22:%5B%22001-182455%22%5D%7D>

⁶⁷ (Chatzinikolaou, 2018), Διαθέσιμο σε: https://strasbourgobservers.com/2018/06/01/benedik-v-slovenia-police-need-a-court-order-to-access-subscriber-information-associated-with-a-dynamic-ip-address/?fbclid=IwZXh0bgNhZW0CMTEAAR0A1Sod9KI-hQHxRewiAqkZ4X0mKgv6wz5BYOt41eg6Z9t0c8FnlYu3YzA_aem_7XSKC6i4MwR4fjOtRao8gQ#_ftn1

⁶⁸ Society for Computers and Law, 2018: <https://www.scl.org/10201-human-rights-judgment-on-accessing-ip-address-information/>

Η απόφαση του Τέταρτου Τμήματος του Δικαστηρίου διερευνά διεξοδικά τη σχέση μεταξύ των δυναμικών διευθύνσεων IP και των δικαιωμάτων προστασίας της ιδιωτικής ζωής. Στην απόφαση αυτή το ΕΔΔΑ δεν κατάφερε να καθιερώσει και να προχωρήσει περαιτέρω την νομολογία του, σχετικά με τα μεταδεδομένα, καθώς δεν επικεντρώθηκε στον ορισμό των δεδομένων προσωπικού χαρακτήρα σε σχέση με τις «δυναμικές διευθύνσεις IP» ούτε στον καθορισμό των κριτηρίων για το πότε μια δυναμική διεύθυνση IP μπορεί να θεωρηθεί δεδομένο προσωπικού χαρακτήρα⁶⁹.

Με την απόφαση αυτή το ΕΔΔΑ τόνισε από την μία πλευρά, την ανάγκη κατάλληλων νομικών εγγυήσεων, όταν οι αρχές επιβολής του νόμου αναζητούν πληροφορίες που εν δυνάμει οδηγούν στην ταυτοποίηση των χρηστών. Από την άλλη, όμως, το Δικαστήριο δεν επιβεβαίωσε πλήρως τη σημασία των μεταδεδομένων, ενώ υποστηρίζεται ότι το Δικαστήριο έχασε την ευκαιρία να εξετάσει με σαφήνεια το ζήτημα της εύλογης προσδοκίας προστασίας της ιδιωτικής ζωής, όσον αφορά τα μεταδεδομένα γενικώς και ειδικότερα τα μεταδεδομένα κίνησης και να εμβαθύνει την νομολογία με τα απαραίτητα κριτήρια που θα εξοπλίσουν την συλλογή των μεταδεδομένων με τις απαραίτητες εγγυήσεις. Στην γνώμη της Δικαστή Yudkivska⁷⁰, στην οποία προσχώρησε και ο δικαστής Bošnjak, επί της αποφάσεως, σημειώνουν πως «Η παρούσα υπόθεση εγείρει το ζήτημα της εύλογης προσδοκίας προστασίας της ιδιωτικής ζωής όσον αφορά τα δεδομένα κυκλοφορίας (μετρήσεις ή μεταδεδομένα) και λυπάμαι που το Δικαστήριο έχασε την ευκαιρία να λάβει σαφή θέση επ' αυτού»⁷¹.

⁶⁹ (Chatzinikolaou, 2018)

⁷⁰ Υπόθεση Benedik κατά Σλοβενίας, Διαθέσιμο σε:

[https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22benedik%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-182455%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22benedik%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-182455%22]})

⁷¹ «Κατά την άποψή μου, αυτή είναι η βασική πρόκληση που πρέπει να διατυπωθεί με σαφήνεια - τα δεδομένα κίνησης ή τα μεταδεδομένα συλλέγονται σήμερα πολύ ευρύτερα από τα δεδομένα περιεχομένου (πραγματικό περιεχόμενο των επικοινωνιών), και η παρέμβαση αυτή πρέπει να «καθορίζεται εκ των προτέρων σε νόμο και να ορίζεται ρητά, εξαντλητικά, επακριβώς και σαφώς, τόσο από ουσιαστική όσο και από διαδικαστική άποψη», καθορίζοντας τις αιτίες και τις προϋποθέσεις που θα επιτρέψουν στο κράτος να υποκλέπτει τις επικοινωνίες των ατόμων, να συλλέγει δεδομένα επικοινωνίας ή «μεταδεδομένα» ή να τα υποβάλλει σε παρακολούθηση ή έλεγχο που εισβάλλει σε σφαίρες στις οποίες έχουν εύλογες προσδοκίες ιδιωτικότητας.»

5.1.8. Breyer κατά Γερμανίας

Η υπόθεση Breyer κατά Γερμανίας⁷² αφορά την περίπλοκη διασταύρωση των δικαιωμάτων προστασίας της ιδιωτικής ζωής. βάσει του άρθρου 8 ΕΣΔΑ και της δυνατότητας του κράτους να έχει πρόσβαση και να διατηρεί μεταδεδομένα για τους σκοπούς της εθνικής ασφάλειας και της επιβολής του νόμου. Η υπόθεση αυτή προέκυψε από την αμφισβήτηση του Christian Breyer κατά του γερμανικού νόμου περί τηλεπικοινωνιών, ο οποίος επέβαλε στους παρόχους τηλεπικοινωνιακών υπηρεσιών να διατηρούν τα «μεταδεδομένα συνδρομητών» όλων των πελατών τους, συμπεριλαμβανομένων εκείνων των οποίων τα στοιχεία δεν είναι απαραίτητα για σκοπούς χρέωσης ή για άλλους συμβατικούς λόγους για συγκεκριμένο χρονικό διάστημα.

Το Δικαστήριο εξέφρασε ανησυχίες, σχετικά με την αναλογικότητα του καθεστώτος διατήρησης δεδομένων, εξετάζοντας το αν η επέμβαση ήταν «αναγκαία σε μια δημοκρατική κοινωνία» καταλήγοντας, όμως, ότι τα δεδομένα αυτά δεν περιείχαν «ιδιαίτερα προσωπικές πληροφορίες ούτε επέτρεπαν τη δημιουργία προφίλ προσωπικότητας ή την παρακολούθηση των κινήσεων των συνδρομητών κινητής τηλεφωνίας, ούτε αφορούσαν μεμονωμένα γεγονότα επικοινωνίας»⁷³.

Η απόφαση δεν αντιμετωπίζει επαρκώς τις ανησυχίες σχετικά με την επάρκεια των εγγυήσεων κατά της κατάχρησης των διατηρούμενων μεταδεδομένων. Σύμφωνα με το ΕΔΔΑ, η γενική διατήρηση δεδομένων συνδρομητών του ιδιωτικού τομέα από την κυβέρνηση, ανεξάρτητα από την ύπαρξη «εύλογων υποψιών» τέλεσης αξιόποινων πράξεως ή πράξεων που βάζουν κατά της εθνικής ασφάλειας, κατά των ατόμων των οποίων τα δεδομένα συλλέγονται, δεν συνιστά παραβίαση της Σύμβασης⁷⁴. Ισχυριζόμενο το Δικαστήριο, ότι η κατοχή και η πρόσβαση από τις αρχές στα δεδομένα συνδρομητών συνιστά αναλογικό μέτρο, καθώς τα δεδομένα αυτά από μόνα τους δεν μπορούν να αποκαλύψουν το προφίλ των χρηστών, προκάλεσε ένα σοβαρό πλήγμα στην έννοια της ανωνυμίας που είναι απαραίτητη για την άσκηση του δικαιώματος στην ιδιωτικότητα.

⁷² Απόφαση Breyer κατά Γερμανίας: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-200442%22%7D>

⁷³ (Vermeulen, 2020), Διαθέσιμο σε: <https://strasbourgobservers.com/2020/03/05/bulk-retention-of-private-sector-subscriber-data-for-governmental-purposes-does-not-violate-the-convention-breyer-v-germany/>

⁷⁴ (Vermeulen, 2020)

Παρατηρούμε, επομένως, συγκρίνοντας την απόφαση αυτή με την απόφαση Big Brothers Watch, πως το ΕΔΔΑ αποφάσισε, ότι τα καθεστώτα μαζικής συλλογής μεταδεδομένων, δεν υπερβαίνουν εγγενώς την ευρεία διακριτική ευχέρεια που παρέχεται στα κράτη-μέλη κατά την επιλογή μεθόδων για την επίτευξη του νόμιμου στόχου της προστασίας της εθνικής ασφάλειας.

Εάν η ευρεία συλλογή λεπτομερών και άκρως παρεμβατικών πληροφοριών είναι επιτρεπτή εντός αυτού του ευρέος περιθωρίου εκτίμησης, όπως στην απόφαση Big Brothers Watch, τότε η διατήρηση δεδομένων συνδρομητών, η οποία είναι συγκριτικά λιγότερο παρεμβατική, είναι ακόμη πιο δικαιολογημένη σύμφωνα με το ΕΔΔΑ. Η απόφαση αυτή υπογραμμίζει τη θέση του Δικαστηρίου, ότι η γενική διατήρηση μεταδεδομένων για κυβερνητικούς σκοπούς είναι αποδεκτή, εφόσον ευθυγραμμίζεται με τους στόχους εθνικής ασφάλειας και εμπίπτει στο νομικό πλαίσιο που έχει θεσπιστεί για τα μέτρα αυτά.

Ο δικαστής Ranzoni στην διαφωνούσα γνώμη του επί της πλειοψηφίας, προέβη στην «αξιολόγηση των εγγυήσεων και κατά πόσον οι υφιστάμενες, εάν υπάρχουν, είναι επαρκείς για την αποτελεσματική πρόληψη της κατάχρησης και της κατάχρησης δεδομένων προσωπικού χαρακτήρα». Επιπλέον, καθώς τα άτομα δεν ενημερώνονται μετά την ανάκτηση των δεδομένων τους, ένα «θύμα της παρέμβασης δεν έχει γνώση και δεν μπορεί να ζητήσει επανεξέταση»⁷⁵.

Το ΕΔΔΑ αποδεχόμενο την ως άνω θέση και παρεκκλίνοντας από την νομολογία του ΔΕΕ για την διατήρηση δεδομένων, θεωρεί επαρκή διασφάλιση της ανωνυμίας του χρήστη το γεγονός, ότι τα δεδομένα συνδρομητών πρέπει να συνδυαστούν με άλλα δεδομένα (όπως κίνησης ή θέσης) για να αποκαλύψουν ευαίσθητα προσωπικά δεδομένα⁷⁶. Η πραγματικότητα, όμως, είναι πως ο νόμος επιτρέπει σε ιδιώτες-παρόχους την γενική και αναιτιολόγητη διατήρηση ταυτοποιήσιμων δεδομένων χρηστών, χωρίς την γνώση τους, άμεσα προσβάσιμα από τις κρατικές αρχές και έτοιμα να φανερώσουν την πλήρη ταυτότητα του χρήστη με μία απλή αντιπαραβολή με μεταδεδομένα κίνησης και θέσης και να συνθέσουν κατ' αυτόν τον τρόπο το πλήρες προφίλ οποιουδήποτε χρήστη,

⁷⁵ Απόφαση Breyer κατά Γερμανίας, διαφωνούσα άποψη από τον δικαστή Ranzoni: [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-200442%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-200442%22])

⁷⁶ Written submissions on behalf of Privacy International and Article 19, Διαθέσιμο σε: <https://privacyinternational.org/taxonomy/term/407>

διευκολύνοντας έτσι την μαζική παρακολούθηση από τις κρατικές αρχές και τις μυστικές υπηρεσίες πληροφοριών.

5.1.8 Ekimdzhiiev και άλλοι κατά Βουλγαρίας

Στην υπόθεση Ekimdzhiiev και άλλοι κατά Βουλγαρίας (11 Ιανουαρίου 2022), εξετάστηκαν κρίσιμα ζητήματα σχετικά με την παρακολούθηση και υποκλοπή επικοινωνιών, με ιδιαίτερη έμφαση στην προστασία των μεταδεδομένων⁷⁷.

Το ΕΔΔΑ αποφάνθηκε υπέρ των προσφευγόντων⁷⁸, κρίνοντας ότι το βουλγαρικό νομικό πλαίσιο δεν παρείχε επαρκείς εγγυήσεις κατά της κατάχρησης. Το ΕΔΔΑ εντόπισε διάφορες ελλείψεις, συμπεριλαμβανομένης της απουσίας αποτελεσματικών ένδικων μέσων για τα άτομα να αμφισβητήσουν την υποκλοπή των επικοινωνιών τους ή τη συλλογή των μεταδεδομένων τους, της ανεπαρκούς δικαστικής εποπτείας για την πρόληψη της αυθαίρετης ή αδικαιολόγητης παρακολούθησης και της έλλειψης σαφών κανόνων σχετικά με τις περιόδους διατήρησης των μεταδεδομένων και τις προϋποθέσεις υπό τις οποίες οι αρχές μπορούσαν να έχουν πρόσβαση στα δεδομένα αυτά⁷⁹.

Το ΕΔΔΑ διαπίστωσε ότι το βουλγαρικό νομικό πλαίσιο δεν διέθετε σαφείς κανόνες σχετικά με τις περιόδους διατήρησης των μεταδεδομένων. Αυτή η απουσία ρύθμισης σήμαινε, ότι τα μεταδεδομένα θα μπορούσαν δυνητικά να διατηρούνται επ' αόριστον, οδηγώντας σε σημαντικό κίνδυνο κατάχρησης και παραβίασης της ιδιωτικής ζωής. Η απόφαση ζητούσε την εφαρμογή ενισχυμένων μηχανισμών εποπτείας, για να διασφαλιστεί, ότι η διατήρηση και η πρόσβαση στα μεταδεδομένα γίνεται εντός των ορίων του νόμου, με τη συμμετοχή δικαστικών και ανεξάρτητων εποπτικών οργάνων για την παρακολούθηση της συμμόρφωσης. Μετά την απόφαση η Βουλγαρία κλήθηκε να τροποποιήσει τη νομοθεσία της για να θεσπίσει κανόνες για τη διατήρηση των μεταδεδομένων, καθορίζοντας συγκεκριμένες περιόδους διατήρησης που είναι αναλογικές

⁷⁷ Περίληψη απόφασης Ekimidzhiev κατά Βουλγαρίας, Διαθέσιμο σε: <https://www.statewatch.org/media/3031/bg-echr-secret-surveillance-aip-legal-summary-11-01-22.pdf>

⁷⁸ (Dimitrova, 2022) Ανακτήθηκε από: <https://strasbourgobservers.com/2022/03/02/ekimdzhiiev-and-others-v-bulgaria-nothing-new-under-the-sun/>

⁷⁹ ECHR Caselaw.com, Διαθέσιμο σε: <https://www.echrcaselaw.com/en/echr-decisions/secret-surveillance-of-communications-and-unsecured-access-to-personal-data-violation-of-the-right-to-respect-for-private-and-family-life/>

και δικαιολογούνται από νόμιμους σκοπούς, τους οποίους αποτελούν η πρόληψη και η διερεύνηση σοβαρών εγκλημάτων και η διασφάλιση της εθνικής ασφάλειας⁸⁰.

Η απόφαση του ΕΔΔΑ στην υπόθεση *Ekimdzhiev και άλλοι κατά Βουλγαρία*, αν και αποσκοπούσε στην ενίσχυση των εγγυήσεων για την προστασία της ιδιωτικής ζωής, δέχεται επικρίσεις μεταξύ άλλων για την παραχώρηση σημαντικής διακριτικής ευχέρειας στις εθνικές αρχές κατά την εφαρμογή των εν λόγω εγγυήσεων⁸¹. Χωρίς αυστηρές και ομοιόμορφες κατευθυντήριες γραμμές από το δικαστήριο, οι εθνικές αρχές ενδέχεται να ερμηνεύσουν τις απαιτήσεις με τρόπους που δεν προστατεύουν επαρκώς την ιδιωτική ζωή των ατόμων⁸², αμφισβητώντας την αποτελεσματικότητα της απόφασης στον πραγματικό περιορισμό των επιπτώσεων των πρακτικών παρακολούθησης. Το ενδεχόμενο μαζικής παρακολούθησης μέσω της συλλογής και διατήρησης μεταδεδομένων παραμένει σημαντικό ζήτημα, καθώς ακόμη και με δικαστική εποπτεία, η μαζική συλλογή μπορεί να οδηγήσει σε εκτεταμένη παρακολούθηση ατόμων χωρίς επαρκή αιτιολόγηση.

Επιπλέον, η έλλειψη διαφάνειας γύρω από τις πρακτικές επιτήρησης δυσχεραίνει την ικανότητα των ατόμων να γνωρίζουν πότε παραβιάζεται η ιδιωτική τους ζωή και να ζητούν αποτελεσματικά ένδικα μέσα. Η απόφαση δεν αντιμετωπίζει, επίσης, επαρκώς το χρονικό διάστημα για το οποίο θα πρέπει να διατηρούνται τα μεταδεδομένα και δεν καθορίζει περιορισμούς στην πρόσβαση, αυξάνοντας τον κίνδυνο κακής χρήσης και μη εξουσιοδοτημένης πρόσβασης. Η δυνατότητα πρόσβασης στα μεταδεδομένα από διάφορες κυβερνητικές υπηρεσίες και όχι μόνο από τις αρχές επιβολής του νόμου, επιδεινώνει περαιτέρω τις ανησυχίες για την προστασία της ιδιωτικής ζωής, καθώς τα δεδομένα μπορούν να διαμοιραστούν και να χρησιμοποιηθούν πέρα από το αρχικό τους πεδίο, οδηγώντας σε ευρύτερες παραβιάσεις του άρθρου 8 της ΕΣΔΑ⁸³.

5.1.9 *Pietrzak και άλλοι κατά Πολωνία*

Η απόφαση αυτή του ΕΔΔΑ δημοσιεύτηκε στις 28 Μαΐου 2024 και είναι το πιο πρόσφατο νομολογιακό δεδομένο, όσον αφορά στην παραβίαση του άρθρου 8, αναφορικά με τις ανεπαρκείς εγγυήσεις κατά της αυθαιρεσίας και της κατάχρησης στη νομοθεσία σχετικά

⁸⁰ (Dimitrova, 2022)

⁸¹ (Statewatch, 2022), Διαθέσιμο σε: <https://www.statewatch.org/news/2022/january/bulgaria-secret-surveillance-data-could-be-used-for-nefarious-purposes-due-to-lack-of-safeguards-rules-echr/>

⁸² (Birrer, He, Just, 2023), Διαθέσιμο σε: <https://ideas.repec.org/a/eee/telpol/v47y2023i4s0308596123000538.html>

⁸³ (Birrer, He, Just, 2023)

με τα μέτρα για τη μαζική παρακολούθηση, τη διατήρηση δεδομένων επικοινωνιών και την πρόσβαση σε αυτά⁸⁴.

Στις 15 Ιανουαρίου 2016, το πολωνικό Κοινοβούλιο θέσπισε τροποποίηση του αστυνομικού νόμου (Police Act), μαζί με άλλες νομοθετικές διατάξεις, με την οποία θεσπίστηκε καθεστώς μαζικής παρακολούθησης και διατήρησης δεδομένων τηλεπικοινωνιών, ταχυδρομικών και ψηφιακών επικοινωνιών (μεταδεδομένων επικοινωνίας). Η εν λόγω νομοθεσία επέτρεπε τη διατήρηση των εν λόγω δεδομένων για περίοδο δώδεκα μηνών από την ημερομηνία σύνδεσης, διευκολύνοντας την πιθανή μελλοντική πρόσβαση των αρμόδιων εθνικών αρχών. Επεκτείνοντας περαιτέρω αυτά τα μέτρα, στις 10 Ιουνίου 2016 τέθηκε σε ισχύ ο αντιτρομοκρατικός νόμος, ο οποίος εξουσιοδοτούσε την πολωνική Εθνική Υπηρεσία Ασφαλείας (ABW) να διενεργεί μυστικές παρακολουθήσεις σε ξένους υπηκόους που είναι ύποπτοι για συμμετοχή σε τρομοκρατικές δραστηριότητες.

Το ΕΔΔΑ αναγνώρισε, ότι η προσβαλλόμενη νομοθεσία επέβαλε την ευρεία και αδιάκριτη διατήρηση τηλεπικοινωνιακών, ταχυδρομικών και ψηφιακών δεδομένων επικοινωνίας για όλους τους χρήστες υπηρεσιών επικοινωνίας (διατηρούνταν τόσο δεδομένα κίνησης και θέσης όσο και ηλεκτρονικές διευθύνσεις ή και σάιτ τα οποία είχαν επισκεφθεί οι χρήστες). Η γενική διατήρηση επηρέασε τα άτομα των οποίων τα δεδομένα αποθηκεύονταν παρά το γεγονός ότι δεν συγκέντρωναν ενδείξεις ενοχής.

Τα διατηρούμενα δεδομένα, τα οποία αποθηκεύονταν για περίοδο δώδεκα μηνών, ήταν προσβάσιμα στην αστυνομία και τις υπηρεσίες πληροφοριών, επιτρέποντάς τους να χρησιμοποιούν τις πληροφορίες για οποιονδήποτε σκοπό κατά την εκτέλεση των νόμιμων καθηκόντων τους. Έτσι, έκρινε πως η ισχύουσα νομοθεσία στο μέτρο που προέβλεπε την πρόσβαση της αστυνομίας και των υπηρεσιών πληροφοριών στα διατηρούμενα δεδομένα επικοινωνιών με τον τρόπο που περιγράφεται ανωτέρω, ήταν ασυμβίβαστη με το άρθρο 8, λόγω της γενικής διατήρησης και αδιάκριτης αποθήκευσης⁸⁵.

Όσον αφορά στην μυστική παρακολούθηση με βάση τον αντιτρομοκρατικό νόμο, οι ρυθμίσεις του επί της αρχής όριζαν την εφαρμογή του κυρίως σε αλλοδαπούς υπηκόους,

⁸⁴ Pietrzak and Bychawska-Siniarska and Others v. Poland Legal Summary, Διαθέσιμο σε: <https://hudoc.echr.coe.int/eng#%7B%22languageisocode%22:%5B%22ENG%22%5D,%22appno%22:%5B%2272038/17%22,%2225237/18%22%5D,%22documentcollectionid%22:%5B%22CLIN%22%5D,%22itemid%22:%5B%22002-14333%22%5D%7D>

⁸⁵ (Timmer, 2024), Διαθέσιμο σε: <https://ellentimmer.com/2024/07/08/surveillance-28/>

όμως, το πεδίο εφαρμογής του επεκτάθηκε σημαντικά στην πράξη. Έτσι, επέτρεψε στην εθνική υπηρεσία ασφαλείας (ABW) να παρακολουθεί έμμεσα τις επικοινωνίες οποιουδήποτε ατόμου είχε έρθει σε επαφή με άτομα υπό παρακολούθηση, ανεξάρτητα από το αν τα ίδια τα άτομα ήταν άμεσα υποκείμενα παρακολούθησης⁸⁶.

Στην απόφασή του το Δικαστήριο κατέληξε στο συμπέρασμα, ότι η έγκριση των μέτρων μαζικής παρακολούθησης από τον επικεφαλής της ABW, υπό τον οποίο λειτουργούσαν οι υπάλληλοι της υπηρεσίας, και οι επακόλουθες αναθεωρήσεις της επιβολής των εν λόγω μέτρων, που επιβλέπονταν από εκτελεστικούς αξιωματούχους με πολιτικό ρόλο και από έναν εισαγγελέα που δεν είχε επαρκή ανεξαρτησία από την εκτελεστική εξουσία, δεν αποτελούσαν επαρκείς εγγυήσεις έναντι ενδεχόμενων καταχρήσεων.

Σημαντική πτυχή της υπόθεσης αυτής, με το οποίο πρόσφατα ασχολήθηκε και η ελληνική νομολογία, όπως θα αναλυθεί και στην συνέχεια, είναι πως σύμφωνα με την πολωνική νομοθεσία, τα άτομα που έχουν γίνει στόχοι μυστικών επιχειρήσεων πληροφοριών, συμπεριλαμβανομένης της παρακολούθησης και ανάλυσης των τηλεπικοινωνιών και των ψηφιακών επικοινωνιών τους, δεν δικαιούνται καμία πληροφορία σχετικά με τις επιχειρήσεις αυτές. Ακόμη και μετά το τέλος των επιχειρήσεων και αφού δεν έχουν απαγγελθεί ποινικές κατηγορίες, οι πολωνικές υπηρεσίες πληροφοριών δεν υποχρεούνται να αποκαλύπτουν λεπτομέρειες σχετικά με τα δεδομένα που συλλέχθηκαν για τα άτομα αυτά, κατά παραβίαση όχι μόνο του άρθρου 8 αλλά και του άρθρου 13 ΕΣΔΑ. Αυτό που παρατήρησε το ΕΔΔΑ είναι, ότι η εν λόγω νομοθεσία δημιούργησε ουσιαστικά ένα

⁸⁶ Ο αντιτρομοκρατικός νόμος της Πολωνίας θέσπισε ένα καθεστώς *lex specialis* σε σχέση με τις διατάξεις περί μυστικής παρακολούθησης του αστυνομικού νόμου. Βάσει αυτής της νομοθεσίας, η ABW είναι εξουσιοδοτημένη δια νόμου, να διεξάγει μυστική παρακολούθηση αλλοδαπών υπηκόων για μια αρχική περίοδο τριών μηνών χωρίς να απαιτείται προηγούμενη δικαστική άδεια ή εποπτεία από ανεξάρτητο φορέα που δεν συνδέεται με την ABW. Αυτή η απουσία ανεξάρτητης εποπτείας δημιούργησε ανησυχίες σχετικά με το ενδεχόμενο οι υπάλληλοι της ABW να ερμηνεύσουν ευρέως τον νόμο, οδηγώντας ενδεχομένως σε ανεπαρκείς λόγους για την υποκλοπή επικοινωνιών. Οι επιχειρήσεις παρακολούθησης ξεκινούσαν με βάση αποφάσεις του επικεφαλής της ABW, με την εποπτεία του Γενικού Εισαγγελέα και του Υπουργού Κρατικών Ειδικών Υπηρεσιών (πρόκειται για τον **Minister Coordinator of Special Forces- συντονίζει τις επιχειρήσεις των ειδικών υπηρεσιών του Internal Security Agency και του Foreign Intelligence Agency**). Ο δικαστικός έλεγχος αποκτούσε σημασία μόνο εάν τα μέτρα επιτήρησης παρατεινόταν πέραν της αρχικής τριμήνου περιόδου, επιτρέποντας έτσι στους υπαλλήλους της ABW σημαντική ευχέρεια χωρίς εξωτερικό έλεγχο κατά την αρχική φάση εφαρμογής των μέτρων επιτήρησης.

σύστημα με το οποίο σχεδόν σε οποιονδήποτε χρήστη τηλεπικοινωνιών ή διαδικτύου θα μπορούσαν να υποκλαπούν τα δεδομένα του εν αγνοία του⁸⁷.

5.2 Νομολογία ΔΕΕ

5.2.1 Απόφαση Digital Rights Ireland και άλλοι

Η απόφαση για τα ψηφιακά δικαιώματα της Ιρλανδίας⁸⁸ (8 Απριλίου 2014) επηρέασε βαθιά το πλαίσιο της διατήρησης δεδομένων στην Ευρωπαϊκή Ένωση, απαιτώντας σημαντικές νομοθετικές και πρακτικές μεταρρυθμίσεις, καθώς αμφισβήτησε τη νομιμότητα της οδηγίας της ΕΕ για τη διατήρηση δεδομένων (Οδηγία 2006/24/EK- Data Retention Directive). Η εν λόγω οδηγία απαιτούσε τη διατήρηση τηλεπικοινωνιακών μεταδεδομένων για χρονικά διαστήματα που κυμαίνονταν από έξι μήνες έως δύο έτη για τους σκοπούς της επιβολής του νόμου.

Το Δικαστήριο, που συνεδρίασε ως τμήμα μείζονος συνθέσεως, έκρινε την οδηγία άκυρη. Οι δικαστές του Λουξεμβούργου διαπίστωσαν ότι οι υποχρεώσεις διατήρησης δεδομένων που προβλέπονται από την Οδηγία συνιστούν «παρέμβαση» στο δικαίωμα στην ιδιωτική ζωή. Επιπλέον, οι κανόνες που διέπουν την πρόσβαση από τις εθνικές αρχές στα διατηρούμενα δεδομένα θεωρήθηκαν «περαιτέρω» επέμβαση στο δικαίωμα αυτό. Το Δικαστήριο έκρινε, ότι η Οδηγία προβλέποντας την επεξεργασία δεδομένων προσωπικού χαρακτήρα, προσέβαλε το δικαίωμα στην προστασία των προσωπικών δεδομένων. Χαρακτήρισε τις παρεμβάσεις αυτές ως «εκτεταμένες» και «ιδιαίτερα σοβαρές» και σημείωσε, ότι ήταν πιθανό να δημιουργήσουν μια διάχυτη αίσθηση στα άτομα ότι η ιδιωτική τους ζωή βρισκόταν υπό συνεχή παρακολούθηση⁸⁹.

Οι σοβαρές επιπτώσεις της απόφασης σε νομικά μέσα και εργαλεία πολιτικής της ΕΕ που ασχολούνται με τη μαζική συλλογή δεδομένων, ήταν τα υφιστάμενα μέτρα και οι προτάσεις της ΕΕ που προβλέπουν «συλλογή μαζικών δεδομένων, αποθήκευση των δεδομένων ενός πολύ μεγάλου αριθμού ανυποψίαστων προσώπων, καθώς και πρόσβαση και χρήση αυτών των δεδομένων από τις αρχές επιβολής του νόμου δεν έχουν σοβαρές

⁸⁷ (Pila, 2024), Ανακτήθηκε από: <https://www.pila.ie/resources/bulletin/2024/06/05/european-court-of-human-rights-rules-polish-secretsurveillance-regime-violates-european-convention-on-human-rights>

⁸⁸ [Digital Rights Ireland and Others, CURIA](#)

⁸⁹ [Council of the European Union, Judgment of the Court of 8 April 2014 and invalidation of the Directive 2006/24, 9009/14, 5 May 2014, Brussels](#)

πιθανότητες να περάσουν τον έλεγχο νομιμότητας» αν δεν συνοδεύονται από υψηλό επίπεδο προστασίας των δεδομένων και «επαρκείς εγγυήσεις για να διασφαλιστεί ότι κάθε σοβαρός περιορισμός των θεμελιωδών δικαιωμάτων περιορίζεται στο απολύτως αναγκαίο και αποφασίζεται στο πλαίσιο των εγγυήσεων που αποτελούν μέρος της νομοθεσίας της Ένωσης αντί να επαφίεται στη νομοθεσία των κρατών μελών»⁹⁰. Κατά συνέπεια, τα κράτη μέλη της ΕΕ υποχρεώθηκαν να επανεξετάσουν και ενδεχομένως να τροποποιήσουν την εθνική τους νομοθεσία που απορρέει από την ακυρωθείσα οδηγία.

Επιπλέον, το Δικαστήριο δήλωσε ότι ο στόχος της καταπολέμησης του σοβαρού εγκλήματος, όσο θεμελιώδης και αν είναι, δεν δικαιολογεί από μόνος του ότι ένα μέτρο που προβλέπει τη γενική και αδιάκριτη διατήρηση όλων των δεδομένων κίνησης και θέσης, όπως αυτό που θέσπιζε η οδηγία 2006/24/EK, πρέπει να θεωρείται αναγκαίο.

Το ΔΕΕ με αυτή την απόφαση πήρε μία σταθερή και ξεκάθαρη θέση απέναντι στις αδιάκριτες και γενικές εντολές διατήρησης δεδομένων και αποτέλεσε κρίσιμο προηγούμενο για μελλοντικές υποθέσεις που σχετίζονται με τη διατήρηση δεδομένων και την επιτήρηση, επηρεάζοντας μεταγενέστερες αποφάσεις, όπως οι υποθέσεις *Tele2 Sverige* και *Watson*.

5.2.2 *Tele2 Sverige AB κατά Post-och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis*

Η απόφαση⁹¹ (21 Δεκεμβρίου 2016) εκδόθηκε μετά από προδικαστικά ερωτήματα της Σουηδίας και του Ηνωμένου Βασιλείου στο ΔΕΕ. Συγκεκριμένα, το Court of Appeal του Ηνωμένου Βασιλείου και το Administrative Court of Appeal της Στοκχόλμης⁹² αναζήτησαν

⁹⁰ (Guild, Carrera, 2014), Διαθέσιμο σε: <https://www.ceps.eu/ceps-publications/political-and-judicial-life-metadata-digital-rights-ireland-and-trail-data-retention/>

⁹¹ *Tele2 Sverige AB (C-203/15) κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis*

⁹² Μετά την απόφαση *Digital Rights Ireland*, και την κατά συνέπεια ακύρωση της Οδηγίας για τη διατήρηση δεδομένων, ως υπερβολική παραβίαση των θεμελιωδών δικαιωμάτων, προέκυψαν νομικές προκλήσεις στη Σουηδία και το Ηνωμένο Βασίλειο. Στη Σουηδία, ο τηλεπικοινωνιακός πάροχος *Tele2 Sverige* σταμάτησε τη διατήρηση δεδομένων των χρηστών της, με την αιτιολογία της μη συμμόρφωσης με την ευρωπαϊκή νομοθεσία, με συνεπακόλουθο την καταγγελία της από το Εθνικό Αστυνομικό Συμβούλιο. Η Σουηδική Αρχή Ταχυδρομείων και Τηλεπικοινωνιών (PTS) διέταξε την *Tele2 Sverige* να συνεχίσει τη διατήρηση δεδομένων, γεγονός που οδήγησε την υπόθεση στην κρίση των Σουηδικών Δικαστηρίων. Με τη σειρά τους, το Διοικητικό Εφετείο της Στοκχόλμης

από το ΔΕΕ προδικαστική απόφαση, σχετικά με την ερμηνεία της ευρωπαϊκής οδηγίας 2002/58/EK για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών υπό το πρίσμα των άρθρων 7 (δικαίωμα στην ιδιωτική ζωή) και 8 (δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα) του ΧΘΔΕΕ. Ειδικότερα, τα εθνικά δικαστήρια διερωτήθηκαν αν το άρθρο 15 της οδηγίας πρέπει να ερμηνευθεί υπό την έννοια ότι απαγορεύει την εθνική νομοθεσία που προβλέπει τη γενική και αδιάκριτη διατήρηση όλων των δεδομένων κίνησης και θέσης όλων των συνδρομητών και εγγεγραμμένων χρηστών όλων των μορφών ηλεκτρονικών επικοινωνιών για τους σκοπούς της καταπολέμησης του εγκλήματος.

Σύμφωνα με την νομολογία του ΔΕΕ και την Digital Rights Ireland, αυτό θα δικαιολογούνταν από λόγους όπως η εθνική ασφάλεια, η άμυνα, η δημόσια ασφάλεια και η πρόληψη, διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων, συμπεριλαμβανομένης της μη εξουσιοδοτημένης χρήσης συστήματος ηλεκτρονικών επικοινωνιών. Επιπλέον, το Δικαστήριο εξέτασε κατά πόσον ένας τέτοιος περιορισμός αποτελεί αναγκαίο, κατάλληλο και αναλογικό μέτρο.

Το Δικαστήριο ανέφερε, ότι η υπό εξέταση νομοθεσία προέβλεπε τη γενική και αδιάκριτη διατήρηση όλων των δεδομένων κίνησης και θέσης όλων των συνδρομητών και εγγεγραμμένων χρηστών που αφορούν όλα τα μέσα ηλεκτρονικής επικοινωνίας και ότι επέβαλε στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών την υποχρέωση να διατηρούν τα δεδομένα αυτά συστηματικά και συνεχώς, χωρίς εξαιρέσεις⁹³.

Το ΔΕΕ παρατήρησε, ότι το εύρος της επιτρεπόμενης παρέμβασης ήταν σημαντικό και μπορούσε να δικαιολογηθεί μόνο από τον στόχο της καταπολέμησης σοβαρών εγκληματικών δραστηριοτήτων, συμπεριλαμβανομένου του οργανωμένου εγκλήματος και της τρομοκρατίας. Ωστόσο, το Δικαστήριο σημείωσε, ότι ο στόχος αυτός από μόνος του δεν

(Stockholm Administrative Court of Appeal) όπως και το Εφετείο του Ηνωμένου Βασιλείου⁹² (U.K. Court of Appeal), παρέπεμψαν στο ΔΕΕ ως προδικαστικό ερώτημα, κατά πόσον μια ευρεία εντολή διατήρησης δεδομένων ήταν συμβατή με το δίκαιο της ΕΕ, λαμβάνοντας υπόψη την προστασία των θεμελιωδών δικαιωμάτων της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων, σύμφωνα με την Οδηγία για την διατήρηση των δεδομένων 2002/58 και συγκεκριμένα το άρθρο 15 παρ.1.

⁹³ (GDPR HUB) CJEU - C 203/15 and C 698/15 - Tele2/Watson (Joined Cases)

Διαθέσιμο σε: [https://gdprhub.eu/index.php?title=CJEU - C 203/15 and C 698/15 - Tele2/Watson \(Joined Cases\)](https://gdprhub.eu/index.php?title=CJEU - C 203/15 and C 698/15 - Tele2/Watson (Joined Cases))

δικαιολογεί επαρκώς την εθνική νομοθεσία που επιβάλλει τη γενική και αδιάκριτη διατήρηση όλων των δεδομένων κίνησης και θέσης. Μια τέτοια νομοθεσία επηρεάζει όλους τους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων εκείνων που δεν ήταν πιθανό να εμπλέκονται σε εγκληματικές δραστηριότητες⁹⁴. Ως εκ τούτου, οι εν λόγω περιορισμοί των θεμελιωδών δικαιωμάτων δεν περιορίζονταν προφανώς στο απολύτως αναγκαίο.⁹⁵

Εν κατακλείδι, το Δικαστήριο καθόρισε τις κατευθυντήριες γραμμές για τη διαδικασία που πρέπει να ακολουθούν οι εθνικές αρχές προκειμένου να διασφαλιστεί η πλήρης τήρηση των εν λόγω προϋποθέσεων. Ανέφερε ότι, εκτός από τις περιπτώσεις νομίμως τεκμηριωμένου επείγοντος, είναι απαραίτητο η πρόσβαση των εθνικών αρχών στα διατηρούμενα δεδομένα να υπόκειται σε προηγούμενο έλεγχο που διενεργείται είτε από δικαστήριο είτε από ανεξάρτητο διοικητικό όργανο και ότι η απόφαση του εν λόγω δικαστηρίου ή οργάνου, πρέπει να έχει ληφθεί κατόπιν αιτιολογημένου αιτήματος των αρχών, που υποβάλλεται στο πλαίσιο των διαδικασιών πρόληψης, ανίχνευσης ή δίωξης του εγκλήματος.

Επιπλέον, οι αρμόδιες εθνικές αρχές στις οποίες είχε χορηγηθεί πρόσβαση στα διατηρούμενα δεδομένα, όφειλαν να ενημερώσουν τα θιγόμενα πρόσωπα, σύμφωνα με τις εφαρμοστέες εθνικές διαδικασίες, μόλις η εν λόγω ενημέρωση δεν ήταν πλέον ικανή να θέσει σε κίνδυνο τις έρευνες που διεξάγονται από τις εν λόγω αρχές. Η κοινοποίηση αυτή ήταν απαραίτητη για να μπορέσουν τα θιγόμενα πρόσωπα να ασκήσουν το δικαίωμά τους για έννομη προστασία. Το Δικαστήριο ανέφερε ότι τα κράτη μέλη πρέπει να διασφαλίζουν τη διενέργεια ανεξάρτητου ελέγχου για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας που εγγυάται το δίκαιο της ΕΕ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

5.2.3 Prokuratuur C-746/18

Η απόφαση⁹⁶ (2 Μαρτίου 2021) αυτή του ΔΕΕ αφορά τους όρους πρόσβασης σε διατηρημένα μεταδεδομένα επικοινωνίας για λόγους καταπολέμησης ιδιαίτερα σοβαρών εγκλημάτων

⁹⁵ (Columbia Global Freedom of Expression, 2016) Διαθέσιμο σε:

<https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/>

⁹⁶ [Prokuratuur C-746/18](#)

και για λόγους εθνικής ασφάλειας, από τις αρχές που είναι αρμόδιες για την έναρξη της δίωξης καθώς και την ανεξαρτησία αυτών.

Το Ανώτατο Δικαστήριο της Εσθονίας ζήτησε διευκρινίσεις από το ΔΕΕ σχετικά με την ερμηνεία του άρθρου 15 παράγραφος 1 της οδηγίας 2002/58/ΕΚ, αφού το Εφετείο απέρριψε τον ισχυρισμό ενός κατηγορουμένου, ότι τα αποδεικτικά στοιχεία αποκτήθηκαν με αθέμιτο τρόπο. Ο κατηγορούμενος, ο οποίος καταδικάστηκε σε φυλάκιση δύο ετών για κλοπή και βία, αμφισβήτησε τη χρήση των δεδομένων ηλεκτρονικών επικοινωνιών, τα οποία διατηρούνται αδιακρίτως και εκτενώς σύμφωνα με την εσθονική νομοθεσία για ένα έτος.

Ο σκοπός της πρόσβασης στα δεδομένα πρέπει να είναι σύμφωνος με το άρθρο 15 παράγραφος 1 της Οδηγίας 2002/58 ΕΚ και πρέπει να καθορίζονται τόσο οι υλικές όσο και οι διαδικαστικές προϋποθέσεις για τη χρήση των δεδομένων. Η γενική πρόσβαση σε όλα τα αποθηκευμένα δεδομένα υπερβαίνει το απολύτως αναγκαίο. Ως εκ τούτου, οι εθνικοί νόμοι πρέπει να διασφαλίζουν ότι οι όροι πρόσβασης καθορίζονται βάσει αντικειμενικών κριτηρίων, περιορίζοντας την πρόσβαση σε δεδομένα κίνησης και θέσης σε περιπτώσεις που αφορούν τη δίωξη σοβαρών ποινικών αδικημάτων, τα συμφέροντα εθνικής ασφάλειας, την εθνική άμυνα ή τη δημόσια ασφάλεια.

Για να πληρούνται αυτές οι απαιτήσεις, η πρόσβαση στα δεδομένα πρέπει να υπόκειται σε προηγούμενο έλεγχο από δικαστήριο ή αρμόδια διοικητική αρχή. Το εν λόγω όργανο επανεξέτασης πρέπει να διαθέτει τις απαραίτητες εξουσίες και εγγυήσεις για την εξέταση των αντικρουόμενων συμφερόντων. Στις ποινικές έρευνες, το όργανο πρέπει να εξισορροπεί την ανάγκη διερεύνησης εγκλημάτων με τα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων. Το όργανο επανεξέτασης πρέπει να ενεργεί αντικειμενικά και αμερόληπτα, χωρίς επιρροή από άλλα μέρη. Δεν πρέπει να εμπλέκεται στην ίδια την έρευνα και πρέπει να παραμένει ουδέτερο όσον αφορά τα μέρη της ποινικής διαδικασίας.

Αν και οι αρχικές αποφάσεις του δικαστηρίου έδιναν σημαντική έμφαση στην ανάγκη διασφάλισης της ιδιωτικής ζωής, οι μεταγενέστερες αποφάσεις οριοθέτησαν και μετρίασαν τις προϋποθέσεις για τη διατήρηση δεδομένων. Ωστόσο, η παρούσα απόφαση αποκλείει ουσιαστικά οποιαδήποτε περαιτέρω χαλάρωση των εν λόγω απαιτήσεων. Περιορίζει, επίσης, την ερμηνεία του άρθρου 15 σχετικά με την πρόσβαση σε δεδομένα κίνησης και θέσης αποκλειστικά στη διερεύνηση σοβαρών εγκλημάτων.

Ωστόσο, η αρμοδιότητα να ορίζουν τι συνιστά σοβαρό έγκλημα παραμένει στα κράτη μέλη. Αυτό ενέχει τον κίνδυνο ο όρος να ερμηνεύεται ευρέως, κατά τρόπο παρόμοιο με αυτόν που έχει παρατηρηθεί στην ερμηνεία της έννοιας της εθνικής ασφάλειας. Αξίζει, να σημειωθεί, ότι τα συνταγματικά δικαστήρια που αντιμετώπισαν ανάλογα ζητήματα δεν έχουν παράσχει με συνέπεια σαφείς περιγραφές του τι συνιστά σοβαρό έγκλημα.

Όσον αφορά στην πτυχή της απόφασης σχετικά με την Εσθονική Εισαγγελία, η οποία είναι υπεύθυνη για τις έρευνες, το ΔΕΕ έκρινε, ότι η εν λόγω υπηρεσία δεν μπορεί να θεωρηθεί ανεξάρτητη αρχή με πρόσβαση στα αποθηκευμένα δεδομένα. Η πιο κρίσιμη διαδικαστική απαίτηση είναι, ότι ένα δικαστήριο ή μια ανεξάρτητη αρχή πρέπει να αναλαμβάνει την εξέταση των αιτήσεων πρόσβασης στα δεδομένα. Η διάταξη αυτή θα καθίστατο ανενεργή, εάν η αρχή, που είναι αρμόδια για τη διερεύνηση του εγκλήματος, αναλάμβανε τον ρόλο του καθορισμού της πρόσβασης στα δεδομένα.

Ο γενικός εισαγγελέας επισήμανε, επίσης, μια πιθανή οδό για μελλοντική εξέταση: κατά πόσον μια ανεξάρτητη εσωτερική αρχή θα μπορούσε να θεωρηθεί επαρκώς ανεξάρτητη για να λαμβάνει αποφάσεις σχετικά με την πρόσβαση στα δεδομένα. Στην υπό εξέταση υπόθεση, η ανακριτική αρχή ήταν δομημένη με ιεραρχικό τρόπο. Παρά τον σαφή εσωτερικό διαχωρισμό μεταξύ της έρευνας και της λήψης αποφάσεων σχετικά με την πρόσβαση στα δεδομένα, ο διαχωρισμός αυτός μπορεί να μην είναι άμεσα εμφανής σε εξωτερικούς παρατηρητές. Κατά συνέπεια, δεν είναι βέβαιο κατά πόσον μια τέτοια εσωτερική αρχή θα πληρούσε το απαιτούμενο πρότυπο επαρκούς ανεξαρτησίας⁹⁷.

5.2.4 Joined Cases C-339/20 (VD) and C-397/20(SR) και Joined Cases C-793/19 (SpaceNet) and C-794/19 (Telekom Deutschland)

Πρόκειται για 4 πρόσφατες υποθέσεις οι οποίες κατέληξαν σε αποφάσεις που επιβεβαιώνουν την πάγια νομολογία ΔΕΕ, όπως διαμορφώθηκε με τις αποφάσεις Digital Rights Ireland και Tele2 Sverige, σχετικά με την γενικευμένη διατήρηση δεδομένων από παρόχους τηλεπικοινωνιών, για λόγους καταπολέμησης ιδιαίτερα σοβαρών εγκλημάτων.

Συγκεκριμένα, η πρώτη απόφαση⁹⁸(20 Σεπτεμβρίου 2022) για τις υποθέσεις Joined Cases C-339/20 (VD) and C-397/20 (SR) αφορούσε διαδικασία που κινήθηκε από τη γαλλική Αρχή

⁹⁷ (Rovelli, 2021), Διαθέσιμο σε: <https://www.europeanpapers.eu/en/europeanforum/case-prokuratuur-proportionality-and-independence>

⁹⁸ [Joined Cases C-339/20\(VD\) and C-397/20 \(SR\)](#)

Χρηματοπιστωτικών Αγορών (AMF) σχετικά με καταγγελίες για εσωτερική πληροφόρηση, διαφθορά και νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Προκειμένου να διερευνήσει τους ισχυρισμούς αυτούς, η AMF βασίστηκε σε προσωπικά δεδομένα από τηλεφωνικές κλήσεις που πραγματοποιήθηκαν κατά τη διάρκεια υπηρεσιών ηλεκτρονικών επικοινωνιών. Οι ύποπτοι προέβαλαν το επιχείρημα ότι η χρήση των εν λόγω δεδομένων από την AMF, αντιβαίνει στο δίκαιο της Ευρωπαϊκής Ένωσης, προτείνοντας ότι η γαλλική νομοθεσία που επιτρέπει τη γενική και αδιάκριτη διατήρηση των δεδομένων κίνησης για περίοδο ενός έτους είναι ασυμβίβαστη με τους κανονισμούς της ΕΕ για την προστασία της ιδιωτικής ζωής.

Το ΔΕΕ έκρινε, ότι οι κανονισμοί για την κατάχρηση της αγοράς δεν μπορούν να δικαιολογήσουν τη γενική υποχρέωση των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών, να διατηρούν αρχεία δεδομένων κίνησης για ένα έτος για τους σκοπούς της οικονομικής εποπτείας από τις αρχές. Επιβεβαίωσε, περαιτέρω, ότι η γενική και αδιάκριτη διατήρηση δεδομένων κίνησης και θέσης από τους εν λόγω φορείς εκμετάλλευσης, ακόμη και για τους σκοπούς της πρόληψης αδικημάτων κατάχρησης της αγοράς, όπως οι εσωτερικές συναλλαγές, αντιβαίνει στην ευρωπαϊκή νομοθεσία.

Στο ίδιο πνεύμα κινείται και η απόφαση (20 Σεπτεμβρίου 2022) για τις υποθέσεις C-793/19 (SpaceNet) and C-794/19 (Telekom Deutschland)⁹⁹. Συγκεκριμένα, η νομιμότητα του γερμανικού νόμου περί τηλεπικοινωνιών (TKG) αμφισβητήθηκε από τους γερμανικούς παρόχους υπηρεσιών διαδικτύου SpaceNet και Telekom Deutschland. Ο TKG επιβάλλει τη διατήρηση δεδομένων κίνησης και θέσης από τις τηλεπικοινωνίες για αρκετές εβδομάδες προκειμένου να αντιμετωπιστούν σοβαρά ποινικά αδικήματα ή απειλές για την εθνική ασφάλεια. Το ΔΕΕ απεφάνθη, ότι το δίκαιο της ΕΕ απαγορεύει την εθνική νομοθεσία που απαιτεί τη γενική και αδιάκριτη διατήρηση δεδομένων ως προληπτικό μέτρο κατά του σοβαρού εγκλήματος και των απειλών για τη δημόσια ασφάλεια. Ωστόσο, το Δικαστήριο σημείωσε, ότι η εν λόγω διατήρηση μπορεί να είναι επιτρεπτή σε συγκεκριμένες περιπτώσεις, ιδίως όταν ένα κράτος μέλος αντιμετωπίζει σοβαρή απειλή για την εθνική ασφάλεια¹⁰⁰.

⁹⁹ [C-793/19 \(SpaceNet\) and C-794/19 \(Telekom Deutschland\)](#)

¹⁰⁰ (Erotokritou, 2022) Ανακτήθηκε από: <https://accesspartnership.com/access-alert-new-judgments-from-the-court-of-justice-of-the-european-union-on-data-retention-by-providers-of-electronic->

5.3. Ευρωπαϊκή νομολογία και μαζική παρακολούθηση

5.3.1 Σύγκριση νομολογίας ΕΔΔΑ και ΔΕΕ

Το ΔΕΕ και το ΕΔΔΑ συμφωνούν σε σημαντικά σημεία, όσον αφορά τα προγράμματα μαζικής παρακολούθησης, κυρίως ως προς την ανάγκη ύπαρξης εγγυήσεων για την αποφυγή κατάχρησης από τις αρχές και τη διατήρηση των δικαιωμάτων της ιδιωτικής ζωής. Και τα δύο δικαστήρια έχουν τονίσει τη σημασία της εξατομικευμένης και εύλογης υποψίας, δηλαδή να υπάρχει σύνδεση μεταξύ της έρευνας και των δεδομένων που συλλέγονται και να εφαρμόζονται οι πρακτικές παρακολούθησης σε καταρχήν υπόπτους. Επίσης, προτιμούν την κοινοποίηση της παρακολούθησης μετά το πέρας της και τη σαφήνεια στους νόμους που ρυθμίζουν αυτές τις πρακτικές.

Ωστόσο, μετά την υπόθεση Big Brother Watch, το ΕΔΔΑ έχει χαλαρώσει την απαίτηση της εκ των υστέρων κοινοποίησης λόγω της φύσης της μαζικής παρακολούθησης και φαίνεται να δίνει μεγαλύτερη έμφαση στην αξία της για λόγους εθνικής ασφάλειας, παρακάμπτοντας την ανησυχία για την δυσκολία προβλεψιμότητας αυτών των προγραμμάτων μαζικής παρακολούθησης. Η στροφή προς πιο τυποποιημένα πρότυπα στους εκάστοτε διαδικαστικούς ελέγχους εισάγει ένα στοιχείο αστάθειας στο πλαίσιο της ΕΣΔΑ. Αυτά τα πρότυπα είναι γνωστά για την ευελιξία τους, κάτι που μπορεί να οδηγήσει ευκολότερα σε ασυνέπειες στη νομολογία.

Παρ' όλο που το νομικό πλαίσιο συνεχίζει να εξελίσσεται, ιδιαίτερα υπό το πρίσμα των μεταβαλλόμενων γεωπολιτικών ανησυχιών για την τρομοκρατία, η εξέλιξη της νομολογίας του ΕΔΔΑ δείχνει ότι το ΔΕΕ παραμένει πιο αφοσιωμένο στην τήρηση των ήδη θεσπισμένων κανόνων. Αυτό είναι σε ευθυγράμμιση και με τα βασικά κείμενα που προστατεύουν τα ατομικά δικαιώματα και τα οποία κάθε δικαστήριο καλείται να ερμηνεύσει. Από την μία η ΕΣΔΑ, η οποία είναι ένα παλαιότερο κατά 50 χρόνια κείμενο, πολύ πριν ανακύψουν οι ανησυχίες του ψηφιακού κόσμου, όπου η προστασία των προσωπικών δεδομένων εντάσσεται στην ευρύτερη προστασία του δικαιώματος στην ιδιωτική ζωή. Από την άλλη το ΔΕΕ ερμηνεύει τον Χάρτη των Θεμελιωδών Δικαιωμάτων, ο

[communications/?fbclid=IwZXh0bgNhZW0CMTEAAR1wnwIS1ArNJ_eYCn9muyXMpkmo9KenMCHnm_aEfvs_BsBI_ryP4SDf5vo_aem_Ipski_ASywFdbDk5_ourKw](https://www.courtenet.europa.eu/communications/?fbclid=IwZXh0bgNhZW0CMTEAAR1wnwIS1ArNJ_eYCn9muyXMpkmo9KenMCHnm_aEfvs_BsBI_ryP4SDf5vo_aem_Ipski_ASywFdbDk5_ourKw)

οποίος ενσωματώνει ρητά ρυθμίσεις για την προστασία των ψηφιακών προσωπικών δεδομένων, γεγονός που ίσως εξηγεί την ανάπτυξη σαφέστερων και σταθερών θέσεων από το ΔΕΕ.

5.3.2. Η θέση της ευρωπαϊκής νομολογίας για την μαζική παρακολούθηση και την γενική διατήρηση μεταδεδομένων

Βάσει της ανάλυσης της ευρωπαϊκής νομολογίας, μπορούν να εξαχθούν ουσιώδη συμπεράσματα σχετικά με την πορεία που ακολουθούν τα Ευρωπαϊκά Δικαστήρια, όσον αφορά στις κατευθυντήριες γραμμές για τις πρακτικές μαζικής παρακολούθησης, ειδικότερα σε σχέση με τις άρσεις του απορρήτου και τη διατήρηση των μεταδεδομένων.

Η πρόσφατη εξέλιξη της νομολογίας των ευρωπαϊκών δικαστηρίων σχετικά με τη μαζική παρακολούθηση καταδεικνύει μια σαφή μεταστροφή προς την αποδοχή μεθόδων συλλογής και επεξεργασίας δεδομένων υπό το πρόσχημα της «εθνικής ασφάλειας». Αυτή η τάση αντικατοπτρίζει τις αυξανόμενες απαιτήσεις των υπηρεσιών πληροφοριών και των αρχών επιβολής του νόμου με πρόφαση την αντιμετώπιση της τρομοκρατίας και του οργανωμένου εγκλήματος. Αντί να απορρίπτονται οι σχετικές προτάσεις άρσεων ως παραβιάσεις των ατομικών δικαιωμάτων, παρατηρείται μια τάση νομιμοποίησης των μεθόδων παρακολούθησης με την προϋπόθεση τήρησης υποτιθέμενων διαδικαστικών εγγυήσεων.

Με την ικανοποίηση των απαιτήσεων των υπηρεσιών πληροφοριών και επιβολής του νόμου, τα ανώτατα δικαστήρια της Ευρώπης εξομαλύνουν τη μαζική παρακολούθηση για λόγους εθνικής ασφάλειας και την κατάργηση της διαδικτυακής ανωνυμίας για σκοπούς επιβολής του νόμου. Τα τελευταία χρόνια, η Ευρώπη έχει γίνει μάρτυρας μιας αξιοσημείωτης τάσης τόσο στον νομοθετικό όσο και στον δικαστικό τομέα, όσον αφορά τα παρεμβατικά μέτρα των μεθόδων των μυστικών υπηρεσιών πληροφοριών και των πάσης φύσεως ερευνητικών μεθόδων. Αντί να απαγορεύονται αρχικά τα μέτρα αυτά, παρατηρείται μια στροφή προς την άδειά τους υπό το πρόσχημα διαδικαστικών και τεχνικών εγγυήσεων¹⁰¹.

Ωστόσο, η προσέγγιση αυτή συχνά μεταφράζεται σε απλές διατυπώσεις, όπου οι υποτιθέμενες εγγυήσεις γίνονται συμβολικές χειρονομίες εποπτείας και όχι ισχυρή

¹⁰¹ (Sajfert, 2021)

προστασία των ατομικών δικαιωμάτων. Η εξέλιξη αυτή εγείρει θεμελιώδη ερωτήματα σχετικά με την ισορροπία μεταξύ των επιταγών της εθνικής ασφάλειας και της διατήρησης των ατομικών ελευθεριών, καθώς και την αποτελεσματικότητα των δικαστικών μηχανισμών στον έλεγχο και τον περιορισμό των κρατικών πρακτικών παρακολούθησης. Άλλωστε και η ίδια η ιδέα της «ισορροπίας» μεταξύ «ιδιωτικότητας» και «ασφάλειας» είναι από μόνη της παραπλανητική: πρώτον, επειδή η επιτήρηση επηρεάζει πολύ περισσότερο από την παραδοσιακή ιδιωτικότητα και, δεύτερον, επειδή ούτε η έννοια της ιδιωτικότητας ούτε η έννοια της ασφάλειας είναι τόσο απλή όσο συχνά παρουσιάζεται. Τα μέτρα για την προστασία της ιδιωτικής ζωής μπορεί να βελτιώνουν την «ασφάλεια» - και τα μέτρα που υποτίθεται ότι βελτιώνουν την ασφάλεια μπορεί με άλλους τρόπους να μειώνουν στην πραγματικότητα την ασφάλεια αυτή¹⁰².

Καθώς τα μέτρα αυτά διευκολύνονται και εφαρμόζονται όλο και περισσότερο, η πρόκληση παραμένει το κατά πόσον η Ευρώπη μπορεί να διατηρήσει ουσιαστικές εγγυήσεις που προστατεύουν πραγματικά την ιδιωτική ζωή και υποστηρίζουν τις αρχές της δημοκρατίας στην ψηφιακή εποχή.

6. Τα μεταδεδομένα επικοινωνίας στην ελληνική έννομη τάξη

Η ανάλυση του ενωσιακού νομικού πλαισίου για την άρση του απορρήτου και την προστασία των μεταδεδομένων επικοινωνίας, με έμφαση στη συλλογή και επεξεργασία των μεταδεδομένων και τον κρίσιμο ρόλο τους στα συστήματα μαζικής παρακολούθησης, οδήγησε στην αποκρυστάλλωση των κατευθυντήριων γραμμών της Ένωσης, για τη διασφάλιση του δικαιώματος στην ιδιωτική ζωή. Η ερμηνεία της σχετικής νομολογίας από το ΕΔΔΑ και το ΔΕΕ δημιουργεί σαφείς όρους και προϋποθέσεις, οι οποίοι καθορίζουν πότε και υπό ποιες συνθήκες μπορεί να γίνει άρση του απορρήτου. Στο σημείο αυτό, η διερεύνηση του ελληνικού νομικού πλαισίου γίνεται αναγκαία για να διαπιστωθεί κατά πόσο οι εγχώριες ρυθμίσεις ευθυγραμμίζονται με την ενωσιακή νομολογία, λαμβάνοντας υπόψη τόσο τις θεσμικές αρμοδιότητες των αρχών όσο και τις διαδικασίες που προβλέπονται για την άρση του απορρήτου, συμπεριλαμβανομένων των μεταδεδομένων επικοινωνίας και κατ' επέκταση ποιο είναι το σύγχρονο πλαίσιο προστασίας.

¹⁰² (Bernal, 2016), Διαθέσιμο [εδώ](#):

6.1 Άρθρο 19 του Συντάγματος

Σύμφωνα με το άρθρο 19 Σ «1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1.

3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9 Α.»

Σημαντική πτυχή της ερμηνείας του άρθρου 19 Σ είναι ο προσδιορισμός της έννοιας του «απορρήτου», το οποίο είναι καταρχήν ζήτημα πραγματικό. Σημαντικό στοιχείο για τον προσδιορισμό του απορρήτου, αφενός είναι το υποκειμενικό-προσωπικό στοιχείο, κατά το οποίο το επικοινωνούν μέρος θεωρεί το περιεχόμενο και τα μεταδεδομένα της επικοινωνίας του ιδιωτικά και αφετέρου το αντικειμενικό-κοινωνικό στοιχείο, κατά το οποίο η ως άνω προσδοκία μπορεί να θεωρηθεί από το σύνολο της κοινωνίας ως εύλογη (reasonable expectation of privacy κατά την νομολογία του ΕΔΔΑ)¹⁰³.

Υπό το πρίσμα του άρθρου 19, όσον αφορά την έννοια της προστατευόμενης ελεύθερης και απόρρητης επικοινωνίας, το φάσμα προστασίας του άρθρου εκτείνεται και στην άμεση επικοινωνία (δια ζώσης) όσο και κάθε άλλου είδους ή μορφή ανταπόκριση ή εν γένει επικοινωνία, συμπεριλαμβανομένου της επικοινωνίας μέσω δημοσίων ή ιδιωτικών δικτύων παροχής υπηρεσιών επικοινωνιών¹⁰⁴. Το απόρρητο των επικοινωνιών είναι «απολύτως απαραβίαστο». Αντικείμενο προστασίας του άρθρου, δεν είναι το μήνυμα αυτό καθ' αυτό¹⁰⁵ αλλά το απόρρητο του μηνύματος, το οποίο πρόκειται για ένα απόρρητο ευρύτερο από άλλα απόρρητα¹⁰⁶. Το Σύνταγμα προστατεύει την επικοινωνία με οποιοδήποτε τρόπο και αν γίνεται, ανεξάρτητα, δηλαδή, από το μέσο που χρησιμοποιείται. Το επικοινωνιακό μέσο είναι αδιάφορο για την προστασία της επικοινωνίας.

¹⁰³ (Παπαδόπουλος, 2008)

¹⁰⁴ (Παναγοπούλου, 2023), Διαθέσιμο σε: <https://www.syntagmawatch.gr/my-constitution/arthro-19/>

¹⁰⁵ Το μήνυμα προστατεύεται ως τέτοιο από το άρθρο 14 παρ.1 του Συντάγματος

¹⁰⁶ (Τσίρης, 2002)

Επομένως, υπάρχει παραβίαση του απορρήτου του μηνύματος, ανεξάρτητα από το αν αυτή η παραβίαση επιφέρει δυσμενείς συνέπειες στην υποστήριξη και διάδοση μιας γνώμης ή στον φορέα του δικαιώματος¹⁰⁷. Η ελευθερία της επικοινωνίας, συνεπώς, συνίσταται στο ότι κάθε άτομο είναι ελεύθερο να επιλέγει το είδος, το μέσο και τον τρόπο επικοινωνίας¹⁰⁸, η οποία αποτελεί και συνταγματικά έννομο προστατευόμενο αγαθό και θεμέλιος λίθος του προστατευτικού πεδίου του απορρήτου των επικοινωνιών¹⁰⁹.

Η κατοχύρωση του απορρήτου ως «απόλυτα απαραβίαστου» έχει υπάρξει ένα δύσκολος ερμηνευτικά όρος στη θεωρία. Βασική και σημαντική συνέπεια της ερμηνείας του, αποτελεί η λειτουργία του ως κριτήριο κατά τη στάθμιση αγαθών και την επίλυση της σύγκρουσης μεταξύ θεμελιωδών δικαιωμάτων. Κατά την εν λόγω διαδικασία στάθμισης και σε συνδυασμό με το β' εδάφιο της παραγράφου 1 του άρθρου 19 του Συντάγματος, όπου προβλέπονται οι ειδικές εξαιρετικές περιπτώσεις παραβίασης του δικαιώματος, ο όρος «απολύτως» συνηγορεί στην υπεροχή του απορρήτου έναντι άλλων δικαιωμάτων¹¹⁰. Κατά βάση προκρίνεται έναντι όλων των θεμελιωδών δικαιωμάτων που τελούν υπό γενική επιφύλαξη νόμου (όπως η ελευθερία του τύπου στο άρθρο 14Σ) καθώς και αυτών που τελούν υπό ειδική επιφύλαξη νόμου υπό τους όρους του β' εδαφίου του άρθρου 19 παρ.1 Σ. Η υπεροχή του αμβλύνεται, όταν συγκρούεται με την θεμελιώδη αρχή της αξίας του ανθρώπου (άρθρο 2 παρ.1 Σ). Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση αποδοχής καταρχήν απαγορευμένων αποδεικτικών μέσων για την απόδειξη της αθωότητας ενός κατηγορουμένου.

6.2 Μεταδεδομένα της επικοινωνίας και απόρρητο

Η θεωρία, κατά πλειοψηφία, είχε την θέση πως τα μεταδεδομένα της επικοινωνίας υπάγονται στο προστατευτικό πεδίο του «απορρήτου της επικοινωνίας», κάτι που αποτυπώθηκε και από τον νομοθέτη στον νόμο 5002/2022, όπως θα αναλυθεί στην συνέχεια. Εκτός από το ίδιο το περιεχόμενο της επικοινωνίας, λοιπόν, προστατεύονται ως απόρρητα και τα μεταδεδομένα, ως δεδομένα που αποκαλύπτουν ευαίσθητα προσωπικά δεδομένα του χρήστη ικανά να συνθέσουν το προφίλ των χρηστών και να αποκαλύψουν,

¹⁰⁷ (Τσίρης, 2002)

¹⁰⁸ (Παναγοπούλου, 2023)

¹⁰⁹ ΑΠ 1/2001

¹¹⁰ (Παπαδόπουλος, 2008)

εκτός από την ταυτότητά του, πολλά περισσότερα στοιχεία ακόμη και από το ίδιο το περιεχόμενο της επικοινωνίας.

Αρχικά, ο ίδιος ο συντακτικός νομοθέτης δεν διακρίνει την επικοινωνία σε «μήνυμα» και σε «εξωτερικά στοιχεία», ώστε να συναχθεί το συμπέρασμα, ότι προστατεύει το μήνυμα και όχι τα εξωτερικά στοιχεία. Τα εξωτερικά στοιχεία, επίσης, μπορούν να οδηγήσουν μέχρι και στην ανασύνθεση του ίδιου του μηνύματος¹¹¹. Αυτό που προστατεύεται ως απόρρητο εν τέλει είναι το «γεγονός της επικοινωνίας» και οτιδήποτε σχετικό με την επικοινωνία, εκτός από το περιεχόμενο, όπως και οι συνθήκες συνολικά γύρω από τις συνθήκες διεξαγωγής της επικοινωνίας.

Στην προστασία του απορρήτου εντάσσονται πλην όλων των υπολοίπων και τα δεδομένα κίνησης και θέσης, οι οποίοι σαν όροι περιλαμβάνονται στον ευρύτερο εξωτερικά στοιχεία της επικοινωνίας. Η ανάγκη υπαγωγής τους στο προστατευτέο πεδίο του απορρήτου υπαγορεύεται από κοινωνικούς παράγοντες¹¹² καθώς η συλλογή και η περαιτέρω επεξεργασία τους ανασυνθέτει την συμπεριφορά των υποκειμένων της επικοινωνίας, επιτρέποντας έτσι την ανασύνθεση του βιοπορτραίτου του επικοινωνούντος¹¹³.

Πριν την κατοχύρωση του απορρήτου χαρακτήρα των μεταδεδομένων επικοινωνίας με τον ν.5002/2022, την ανωτέρω λογική είχε υιοθετήσει το ΠΔ 47/2005, όπου στο άρθρο 4 παρ.1 είχε ρητά υπαγάγει τα μεταδεδομένα στο απόρρητο της επικοινωνίας. Ακόμη και στον προηγούμενο εκτελεστικό νόμο 2225/1994 συνδυαστικά με το ΠΔ 47/2005 δεν προβλεπόταν η απόκτηση των μεταδεδομένων επικοινωνίας από τους παρόχους χωρίς την τήρηση των απαραίτητων προϋποθέσεων για την άρση του απορρήτου, ήτοι την έκδοση εντάλματος ή βουλεύματος¹¹⁴.

Πριν την ψήφιση του νόμου 5002/2022, είχε επικρατήσει σύγχυση στον νομικό κόσμο, λόγω μιας σειράς Γνωμοδοτήσεων εισαγγελιών του Αρείου Πάγου όπου δεν ενέτασσαν τα εξωτερικά στοιχεία της επικοινωνίας στην συνταγματική προστασία του επικοινωνιακού απορρήτου (η Γνωμοδότηση 9/2009¹¹⁵ του Εισαγγελέα του Αρείου Πάγου Γεωργίου Σανιδά,

¹¹¹ (Παπαδόπουλος, 2008)

¹¹² (Μαυριάς, 1982)

¹¹³ (Παναγοπούλου, 2023)

¹¹⁴ (Παναγοπούλου, 2023)

¹¹⁵ [Γνωμοδότηση 9/2009](#)

η Γνωμοδότηση 12/2009¹¹⁶ του Εισαγγελέα του Αρείου Πάγου Ιωάννη Τεντέ και η Γνωμοδότηση 9/2011¹¹⁷ του αντιεισαγγελέα του Αρείου Πάγου Αθανασίου Κατσιρώδη). Σε αντίθετο πνεύμα κινούνταν η ΑΔΑΕ η οποία είχε γνωμοδοτήσει υπέρ της ερμηνείας σχετικά με την υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στο προστατευτέο απόρρητο της επικοινωνίας (Γνωμοδότηση 1/2005)¹¹⁸.

7. Ανάλυση και κριτική του νόμου 5002/2022

Ο νόμος αυτός ψηφίστηκε με γνώμονα την διαμόρφωση ενός σύγχρονου και αποτελεσματικού νομικού πλαισίου, για την εξασφάλιση της προστασίας του απορρήτου των επικοινωνιών και την κάλυψη των νομοθετικών κενών, λόγω των ταχύτατων τεχνολογικών εξελίξεων στον τομέα των ηλεκτρονικών επικοινωνιών. Υπογραμμίστηκε η ανάγκη για άμεσο εκσυγχρονισμό και λεπτομερή ρύθμιση αυτής της διαδικασίας, τηρώντας την αρχή της αναλογικότητας και το άρθρο 19 του Συντάγματος. Απουσιάζει αναφορά στο ενωσιακό δίκαιο και συγκεκριμένα στο παράγωγο δίκαιο της ΕΕ και στην Οδηγία 2002/58/ΕΚ σχετικά με την πλήρη εναρμόνιση του νέου νομοθετικού πλαισίου, καθώς και σε άλλες νομοθετικές ρυθμίσεις εκτός του προϊσχύσαντος νόμου 2225/1994, με απώτερο στόχο την επίτευξη των ως άνω αναφερόμενων σκοπών. Εξαρχής, λοιπόν, εντοπίζεται ένα σημαντικό έλλειμμα στον νέο νόμο και τις ρυθμίσεις σε αυτόν¹¹⁹.

7.1 Εξωτερικά στοιχεία της επικοινωνίας

Μία από τις θεμελιώδεις αλλαγές του ν. 5002/2022 ήταν η ένταξη των εξωτερικών στοιχείων επικοινωνίας στο προστατευτέο απόρρητο όσον αφορά στην επικοινωνία, εισάγοντας ρητή ρύθμιση στο άρθρο 4 παρ. 4 στοιχείο δ («*Η διάταξη που επιβάλλει την άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας περιέχει: δ) το αντικείμενο της άρσης, δηλαδή τα εξωτερικά στοιχεία της επικοινωνίας ή και το περιεχόμενο αυτής*»), όσον αφορά τις περιπτώσεις άρσης για λόγους εθνικής ασφάλειας και στο άρθρο 6 παρ. 4 στοιχείο ζ («*Το βούλευμα ή η διάταξη που επιβάλλει την άρση του απορρήτου για διακρίβωση εγκλημάτων, περιλαμβάνει: ζ) το αντικείμενο της άρσης, δηλαδή τα εξωτερικά στοιχεία της επικοινωνίας ή και το περιεχόμενο α τής, η) την εδαφική έκταση εφαρμογής, εφόσον*

¹¹⁶ [Γνωμοδότηση 19/2009](#)

¹¹⁷ [Γνωμοδότηση 9/2011](#)

¹¹⁸ [ΑΔΑΕ Γνωμοδότηση 1/2005](#)

¹¹⁹ (Τσόλιας, 2023)

απαιτείται για τις ανάγκες της άρσης, και την απολύτως αναγκαία χρονική διάρκεια της άρσης»), όσον αφορά τις περιπτώσεις άρσης για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Πλέον, στην έννοια της άρσης του απορρήτου εμπίπτει τόσο το περιεχόμενο όσο και τα εξωτερικά στοιχεία της επικοινωνίας ή αλλιώς «μεταδεδομένα επικοινωνίας», εναρμονίζοντας, έτσι, το ελληνικό νομικό πλαίσιο ως προς το ζήτημα αυτό, με την ενωσιακή νομοθεσία αλλά και την πάγια νομολογία του ΕΔΔΑ, του ΔΕΕ καθώς και του ΣτΕ, παρά τις εκπεφρασμένες αντιρρήσεις του Αρείου Πάγου και της Εισαγγελίας, διορθώνοντας έτσι ένα χρόνιο δικαιοκρατικό έλλειμμα. Πλέον για την άρση των μεταδεδομένων επικοινωνίας πρέπει να τηρηθούν οι απαραίτητες διατυπώσεις του νόμου, ανάλογα, με το αν αφορά άρση για λόγους εθνικής ασφάλειας ή για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Παρ' όλα αυτά, ασκείται μία κριτική στην διατήρηση του όρου εξωτερικά στοιχεία επικοινωνίας, σε αντιδιαστολή με το περιεχόμενο αυτής. Οι ταχύτατες τεχνολογικές εξελίξεις στις δικτυακές υποδομές καθιστούν άνευ σημασίας τη διάκριση, μεταξύ του περιεχομένου και των εξωτερικών στοιχείων των ηλεκτρονικών επικοινωνιών, καθώς οι πληροφορίες που αντλούνται από τα μεταδεδομένα επικοινωνίας αποτελούν προσωπικά δεδομένα, ικανά για την σύνθεση του προφίλ του χρήστη, καθιστώντας αυτά κάποιες φορές πιο σημαντικά από το ίδιο το περιεχόμενο της επικοινωνίας¹²⁰.

Χαρακτηριστική είναι η πρόβλεψη στην πρόταση Κανονισμού e Privacy σχετικά με την υπαγωγή του περιεχομένου της επικοινωνίας στην νέα προτεινόμενη έννοια «δεδομένα της επικοινωνίας» καταργώντας, έτσι, στην ουσία τον διαχωρισμό περιεχομένου και εξωτερικών στοιχείων επικοινωνίας, τα οποία ονομάζονται «μεταδεδομένα της επικοινωνίας» και υπάγονται με την σειρά τους και αυτά στα δεδομένα της επικοινωνίας¹²¹.

Η κατάργηση του διαχωρισμού κρίνεται απαραίτητη, καθώς αποδεχόμενοι ότι και το περιεχόμενο όσο και τα μεταδεδομένα της επικοινωνίας αποκαλύπτουν πληροφορίες που αποτελούν προσωπικά δεδομένα, ως «δεδομένα επικοινωνίας» πλέον ενεργοποιούν τις διατάξεις του ΓΚΠΔ οι οποίες έχουν άμεση και δεσμευτική ισχύ, σε μια προσπάθεια

¹²⁰ (Τσόλιας, 2023)

¹²¹ (Τσόλιας, 2023)

ενοποίησης του δικαίου και κατανομής ανάλογης προστασίας σε όλα τα στοιχεία της επικοινωνίας.

Επιπλέον, η διάκριση αυτή δεν ανταποκρίνεται στην πρόοδο της τεχνολογίας, ειδικότερα του τρόπου μετάδοσης της επικοινωνίας καθώς και της χρήσης των δικτύων ηλεκτρονικών επικοινωνιών. Οι τεχνολογικές εξελίξεις οδήγησαν στην κατάργηση της μεταφοράς σημάτων και στην αντικατάστασή τους από πρωτόκολλα διαδικτύου IP καθιστώντας ταυτοχρόνως άνευ αντικειμένου τις νομοθετικές διατάξεις που στηρίζονται στην έννοια της «διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας». Κατ' αυτόν τον τρόπο, στο τεχνολογικό επίπεδο, η διάκριση μεταξύ «εσωτερικών» και «εξωτερικών» στοιχείων της επικοινωνίας στο διαδίκτυο έχει καταστεί αδύνατη. Σε αυτό συμβάλλει το γεγονός, ότι ο πάροχος συχνά συνδυάζει διαφορετικά τεχνολογικά συστατικά, όπως τα πρωτόκολλα ip, με τέτοιο τρόπο ώστε αυτό που θεωρείται περιεχόμενο για ένα συστατικό (όπως τα στοιχεία που αποκαλύπτουν την πρόσβαση σε συγκεκριμένη ιστοσελίδα) ταυτόχρονα θεωρείται και «δεδομένο κίνησης»¹²².

7.2 Λόγοι «εθνικής ασφάλειας»

Οι πρόσφατες ρυθμίσεις, σχετικά με την άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας, έχουν εγείρει ανησυχίες σχετικά με τις ευρύτερες επιπτώσεις, σε σχέση με τον επιδιωκόμενο σκοπό του νόμου.

Αρχικά, ένα διαχρονικό ζήτημα είναι ο περιορισμός της έννοιας της εθνικής ασφάλειας ώστε να πληροί και τα κριτήρια που θέτονται από την ευρωπαϊκή νομοθεσία αλλά και να είναι ευκρινής η νομική βάση άρσης του απορρήτου καθώς και τα όρια εξουσίας των αρχών. Ο ορισμός, όμως, όπως περιλαμβάνεται στο άρθρο 3 του ν 5002/2022, είναι ευρύς, αν και πιο στενός από το προτεινόμενο σχέδιο νόμου. Σύμφωνα με αυτό, «Λόγοι εθνικής ασφάλειας είναι οι λόγοι που συνάπτονται με την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων των Ελλήνων πολιτών, όπως, ιδίως, λόγοι σχετικοί με την εθνική άμυνα, την εξωτερική πολιτική, την ενεργειακή ασφάλεια και την κυβερνοασφάλεια». Ο ορισμός δεν είναι πλήρης και δεν συμφωνεί με την πάγια νομολογία του ΕΔΔΑ, η οποία έχει κρίνει, πως η εθνική νομοθεσία για τις μυστικές παρακολουθήσεις οφείλει να είναι επαρκώς σαφής και λεπτομερής, ώστε να ενημερώνει τους πολίτες για τις

¹²² (Τσόλιας, 2023)

συνθήκες και τους όρους υπό τους οποίους, οι δημόσιες αρχές έχουν την εξουσία να εφαρμόζουν τέτοιου είδους μέτρα¹²³.

Στην συνέχεια στο άρθρο 4 παρ.1 του ν. 5002/2022 ρυθμίζεται το αίτημα για την άρση του απορρήτου το οποίο μπορεί να υποβληθεί μόνο από την Ε.Υ.Π ή την Δ.Α.Ε.Ε.Β, είτε με δική τους πρωτοβουλία είτε κατόπιν σχετικού αιτήματος, που διαβιβάζεται από δικαστική ή άλλη πολιτική, στρατιωτική ή αστυνομική δημόσια αρχή στην αρμοδιότητα της οποίας υπάγεται το θέμα εθνικής ασφάλειας που επιβάλλει την άρση.

Το αίτημα πρέπει να περιλαμβάνει συγκεκριμένα στοιχεία που αιτιολογούν τις υποψίες για πρόκληση κινδύνου κατά της εθνικής ασφάλειας που να βασίζονται σε αντικειμενικά δεδομένα. Επομένως, αυτά τα στοιχεία πρέπει να καταγράφονται με σαφήνεια στον νόμο, ώστε να υπάρχει η αναγκαία νομική βάση για την άρση του απορρήτου. Όπως αναφέρθηκε ανωτέρω, στην παράγραφο 2 του άρθρου 4 περιλήφθηκαν για πρώτη φορά τα εξωτερικά στοιχεία της επικοινωνίας σχετικά με το αντικείμενο της άρσης.

Ο νόμος παρά τον σκοπό εκσυγχρονισμού του νομικού πλαισίου για την άρση του απορρήτου, διατήρησε το προϋπάρχον σύστημα της έκδοσης εισαγγελικής διάταξης από τον εισαγγελέα της ΕΥΠ και τον εισαγγελέα της ΔΑΕΕΒ, ο οποίος μέσα σε 24 ώρες κρίνει για την άρση ή όχι και υποβάλλεται κατόπιν η εισαγγελική διάταξη μαζί με το αίτημα και τα συνοδεύοντα αυτό στοιχεία, που ετέθησαν υπόψη του εισαγγελικού λειτουργού, για έγκριση σε δεύτερο εισαγγελικό λειτουργό, ο οποίος είναι αντεισαγγελέας του Αρείου Πάγου ή εισαγγελέας Εφετών και ορίζεται με απόφαση του Εισαγγελέα του Αρείου Πάγου για θητεία ενός (1) έτους.

Η προβληματική που ανακύπτει, είναι, πως παρ' όλη την προσθήκη του δεύτερου εγκριτικού σταδίου δεν θεραπεύεται η παθογένεια του συστήματος, αφού στην πραγματικότητα στηρίζεται σε ένα μονοπρόσωπο όργανο (εισαγγελικός λειτουργός), το οποίο είναι αποσπασμένο από τον φυσικό του χώρο και μόνιμα τοποθετημένο στο περιβάλλον της Ε.Υ.Π και της Δ.Α.Ε.Ε.Β με φυσική απόρροια την ενσωμάτωσή του στην νοοτροπία της υπηρεσίας και την κατάργηση της ανεξαρτησίας αυτού. Υπάρχει ουσιαστική διαφορά όταν ένας κρατικός λειτουργός πρέπει απλώς να εγκρίνει ή να απορρίψει μια απόφαση που έχει ήδη ληφθεί, χωρίς να έχει άλλη επιλογή, σε σύγκριση με το να

¹²³ (Συμεωνίδου-Καστανίδου, 2022) Ανακτήθηκε από: https://www.constitutionalism.gr/to-sxedio-nomou-sxetika-me-tin-arsi-tou-aporitou-ton-epikoinonion/#_ftn3

συμμετέχει εξ αρχής στη διαμόρφωση μιας κοινής απόφασης μαζί με άλλους στο πλαίσιο ενός συλλογικού οργάνου¹²⁴.

Ο χρόνος, επίσης, αποτελεί κρίσιμο παράγοντα, και το χρονικό διάστημα των είκοσι τεσσάρων ωρών είναι εξαιρετικά περιορισμένο, καθιστώντας αδύνατη τη διεξοδική ανάλυση των στοιχείων που θα μπορούσαν να αιτιολογήσουν την άρση του απορρήτου σύμφωνα με την αρχή της αναλογικότητας. Το ζήτημα του χρόνου καθίσταται ακόμη πιο προβληματικό, όταν υπάρχουν πολλαπλά αιτήματα για άρση απορρήτου εντός της ίδιας ημέρας, γεγονός που καθιστά το διαθέσιμο χρονικό πλαίσιο απολύτως ανεπαρκές¹²⁵.

Ένα από τα σημαντικότερα ελλείμματα του νόμου είναι η έλλειψη αιτιολογίας λήψεως του μέτρου άρσης του απορρήτου καθώς και το ονοματεπώνυμο του παρακολουθούμενου (βλ. άρθρο 4 παρ.2) σε αντίθεση με ό,τι ισχύει για την άρση του απορρήτου προς διακρίβωση εγκλημάτων. Η σημασία της αιτιολογίας έγκειται στο ότι επιτρέπει την αξιολόγηση των ενεργειών κάθε κρατικού οργάνου, είτε πρόκειται για διοικητικό είτε για δικαστικό, όσον αφορά τη συμμόρφωσή τους με το νόμο, την τήρηση ή υπέρβαση των ορίων της διακριτικής τους ευχέρειας, την αποφυγή αυθαιρεσιών και κατάχρησης εξουσίας, καθώς και τη λήψη αποφάσεων σύμφωνα με την αρχή της αναλογικότητας ενώ είναι και η βάση της λογοδοσίας αυτού του οργάνου. Ταυτοχρόνως αποτελεί δικαίωμα των διοικουμένων η αιτιολόγηση των δυσμενών αποφάσεων των κρατικών οργάνων και θεμελιώδης αρχή του κράτους δικαίου¹²⁶.

Η απουσία αναφοράς ονόματος, περαιτέρω, σε συνδυασμό με τη σαφή αναφορά στην «εδαφική έκταση εφαρμογής» της άρσης στο άρθρο 4 παρ. 4 (δ) του νόμου, υποδηλώνει ότι το νέο νομικό πλαίσιο μπορεί να επιτρέπει μαζικές παρακολουθήσεις για λόγους εθνικής ασφάλειας, πρακτική η οποία δεν είναι απαγορευμένη από το ΕΔΔΑ και εμπίπτει στις

¹²⁴ ΑΔΑΕ Δελτίο Τύπου - Περίληψη των πλέον σημαντικών παρατηρήσεων επί του νομοσχεδίου για την διαδικασία άρσης απορρήτου των Επικοινωνιών, την κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων, 2022, Ανακτήθηκε από: <https://adae.gov.gr/enimerosi/deltia-typou/perilepse-ton-pleon-semantikon-paratereseon-epi-tou-nomoschediou-gia-ten-diadikasia-arses-aporretou-ton-epikoinonion-ten-kybernoasphaleia-kai-ten-prostasia-prosopikon-dedomenon>

¹²⁵ (Συμεωνίδου-Καστανίδου, 2022)

¹²⁶ (ΑΔΑΕ Δελτίο Τύπου, 2022) Ανακτήθηκε από: <https://adae.gov.gr/enimerosi/deltia-typou/perilepse-ton-pleon-semantikon-paratereseon-epi-tou-nomoschediou-gia-ten-diadikasia-arses-aporretou-ton-epikoinonion-ten-kybernoasphaleia-kai-ten-prostasia-prosopikon-dedomenon>

αρμοδιότητες των κρατών-μελών σύμφωνα με αυτό. Καθώς, όμως, οι μαζικές παρακολουθήσεις ενέχουν αυξημένο κίνδυνο παραβίασης των θεμελιωδών ελευθεριών ατόμων που δεν αποτελούν καμία απειλή για την εθνική ασφάλεια το ΕΔΔΑ απαιτεί συγκεκριμένες εγγυήσεις για την αποφυγή της κατάχρησης.

Εάν το κράτος δεν προτίθεται να υιοθετήσει μεθόδους μαζικής παρακολούθησης, οι εισαγγελικές διατάξεις πρέπει να αναφέρουν το όνομα του ατόμου που θα παρακολουθείται και να αιτιολογούν πλήρως τους λόγους για την παρακολούθηση, όπως συμβαίνει στις υποθέσεις διακρίβωσης εγκλημάτων, με απώτερο σκοπό τον έλεγχο της νομιμότητας από την ΑΔΑΕ, ως της συνταγματικά καθορισμένης αρχής με ρόλο «αντίβαρου εξουσίας» στην δικαστική αρχή¹²⁷.

Αντιθέτως, αν εφαρμόζεται ή συνεχίζεται η χρήση πρακτικών μαζικής παρακολούθησης από τις κρατικές υπηρεσίες σύμφωνα με την νομολογία του ΕΔΔΑ και του ΔΕΕ πρέπει να υπάρχει ξεκάθαρη αναφορά στον νόμο με την επακόλουθη υιοθέτηση αυξημένων διασφαλίσεων.

Οι διασφαλίσεις αυτές σύμφωνα με την νομολογία του ΕΔΔΑ περιλαμβάνουν την ρητή και σαφή αναφορά στον εθνικό νόμο των λόγων για τους οποίους μπορεί να επιτρέπεται η άρση του απορρήτου καθώς και τις «διασφαλίσεις από άκρο σε άκρο». Συγκεκριμένα, πρέπει να υπάρχει ένα ευρύ πλέγμα αξιολόγησης και εποπτείας, το οποίο να περιλαμβάνει αξιολόγηση σε κάθε στάδιο της διαδικασίας, οι τακτικές μαζικής παρακολούθησης θα πρέπει να εποπτεύονται από την αρχή της διαδικασίας από μία ανεξάρτητη αρχή καθώς και κατά την πραγματοποίησή της έως και την περαίωσή της ¹²⁸.

Μία από τις θεμελιώδεις αλλαγές του ν. 5002/2022 αφορά την εκ των υστέρων ενημέρωση των θιγόμενων από την διαδικασία άρσης του απορρήτου μόνο μετά την πάροδο 3 ετών από την παύση της ισχύος της διάταξης άρσης του απορρήτου για λόγους εθνικής ασφάλειας. Για πρώτη φορά μετά από 18 χρόνια αφαιρέθηκε η αρμοδιότητα αυτή από την ΑΔΑΕ και ανατέθηκε σε ένα τριμελές όργανο που αποτελείται από τους 2 εισαγγελικούς λειτουργούς (της ΕΥΠ ή τον εισαγγελικό λειτουργό της παρ. 3 του άρθρου 4 του ν. 2265/1994) που εξέδωσαν την απόφαση για την άρση του απορρήτου και από τον πρόεδρο της ΑΔΑΕ.

¹²⁷ (ΑΔΑΕ Δελτίο Τύπου, 2022)

¹²⁸ (Συμεωνίδου-Καστανίδου, 2022)

Σύμφωνα με το ΕΔΔΑ, το όργανο αρμόδιο για την ενημέρωση του θιγόμενου πρέπει να είναι ανεξάρτητο, επομένως δεν θα έπρεπε να συμμετέχουν οι εισαγγελικοί λειτουργοί οι οποίοι αποφάσισαν την επιβολή του μέτρου της άρσης του απορρήτου. Αντιθέτως, μόνη συνταγματικώς αρμόδια σύμφωνα με το άρθρο 19 παρ. 2 Σ, η οποία πληροί και τα απαραίτητα εχέγγυα ανεξαρτησίας είναι η ΑΔΑΕ ως τελικός εγγυητής της τήρησης της νομιμότητας της διαδικασίας άρσης του απορρήτου. Το τριμελές όργανο της παρ. 7 του άρθρου 4, δεν πληροί της προϋποθέσεις ανεξαρτησίας μιας ανεξάρτητης αρχής.

Στην ουσία τα δύο μέλη του οργάνου αυτού, το οποίο μάλιστα αποφασίζει κατά πλειοψηφία, καλούνται να κρίνουν τις συνέπειες των πράξεων που οι ίδιοι αποφάσισαν. Η διαδικασία γνωστοποίησης αφορά την προστασία του δικαιώματος στον ιδιωτικό βίο καθώς και του δικαιώματος προσφυγής στα ένδικα μέσα του θιγόμενου και αυτή η προστασία, δεν είναι δυνατόν να επαφίεται σε εισαγγελικούς λειτουργούς που δρουν μέσα στο πλαίσιο της ΕΥΠ, η οποία στην προκειμένη, είναι η υπηρεσία η οποία πρέπει να ελεγχθεί για ενδεχόμενες καταχρήσεις και για μη τήρηση των απαραίτητων εγγυήσεων, της οποίας, μάλιστα, τα όργανα είναι αυτά που εισηγήθηκαν στον εισαγγελέα την ανάγκη άρσης του απορρήτου για λόγους εθνικής ασφάλειας.

Προβληματικό είναι και το χρονικό διάστημα το οποίο πρέπει να παρέλθει για να ενημερωθεί ο θιγόμενος, το οποίο είναι τρία χρόνια από την παύση της διάταξης. Πρόκειται για ένα πολύ μεγάλο διάστημα, ειδικά στην περίπτωση που δεν έχουν προκύψει ευρήματα περί του κινδύνου για την εθνική ασφάλεια και αντιβαίνει στην νομολογία της ΕΔΔΑ η οποία έχει κρίνει, ότι η ενημέρωση παρέχεται «αμέσως μετά τη λήξη της παρακολούθησης, εφόσον δεν διακυβεύεται πλέον ο σκοπός για τον οποίο διατάχθηκε η λήψη του μέτρου»¹²⁹.

Μείζον ζήτημα αποτελεί, επίσης, το γεγονός πως η γνωστοποίηση δεν είναι πλήρης, καθώς γνωστοποιείται στον θιγόμενο μόνο η επιβολή του περιοριστικού μέτρου και η διάρκειά του και όχι οι λόγοι για τους οποίους επιβλήθηκε το μέτρο αυτό. Η πρόβλεψη αυτή καταργεί τον πυρήνα του δικαιώματος της γνωστοποίησης, έτσι, όπως έχει κριθεί και κατά την νομολογία του ΕΔΔΑ αλλά και κατά την ελληνική έννομη τάξη, ο οποίος είναι η δυνατότητα του θιγόμενου να προσφύγει στην κατάλληλη ένδικη προστασία. Χωρίς την γνώση της αιτιολογίας του μέτρου της άρσης, ο θιγόμενος δεν μπορεί να ασκήσει

¹²⁹ Roman Zakharov v. Russia

αποτελεσματικά το δικαίωμα σε δικαστική προστασία, όπως υπαγορεύει το Σύνταγμα στο άρθρο 20 παρ.1, καθώς και το άρθρο 13 της ΕΣΔΑ.

Τέλος, ελλειμματική είναι η πρόβλεψη, πως απαιτείται η υποβολή σχετικού αιτήματος στην ΑΔΑΕ, το οποίο στην συνέχεια διαβιβάζεται στην Ε.Υ.Π και την Δ.Α.Ε.Ε.Β. Η διάταξη αυτή αγγίζει τα όρια του παραλόγου, καθώς αφορά μία μυστική παρακολούθηση την οποία ο άμεσα ενδιαφερόμενος εξ ορισμού δεν μπορεί να γνωρίζει, ούτε υπάρχει η πρόβλεψη ώστε να μπορεί να απευθύνει κάπου μία σχετική ερώτηση για το αν παρακολουθείται ή όχι. Η ρύθμιση αυτή αντιβαίνει για άλλη μία φορά την νομολογία του ΕΔΔΑ σύμφωνα με την οποία η ενημέρωση θα πρέπει να παρέχεται από μία ανεξάρτητη αρχή στον θιγόμενο αμέσως μετά την λήξη του μέτρου της άρσης και εφόσον δεν διακυβεύεται ο σκοπός λήψης αυτού.

7.3 Άρση για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων

Στο άρθρα 6 και 7 του ν. 5002/2022, όπου ρυθμίζονται τα σχετικά με την άρση του απορρήτου για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων οι ρυθμίσεις είναι διαφοροποιημένες σε σχέση με το κομμάτι της εθνικής ασφάλειας. Υπήρξαν αλλαγές από το προηγούμενο νομικό καθεστώς του ν. 2225/1994, καθώς και από το σχέδιο νόμου, το οποίο είχε προταθεί προς διαβούλευση.

Ανάμεσα στις βελτιωτικές αλλαγές συμπεριλαμβάνεται η μείωση των εγκλημάτων για τα οποία επιτρέπεται η άρση του απορρήτου για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων στο άρθρο 6 παρ.1,2, και η ρητή αναφορά στο άρθρο 7 παρ.1 της υποχρεωτικής συμπερίληψης στη δικογραφία του υλικού που συλλέχθηκε κατά την άρση του απορρήτου, όχι μόνο για την άσκηση της ποινικής δίωξης του κατηγορουμένου αλλά και για την αθώωση αυτού τηρώντας, έτσι, το τεκμήριο αθωότητας του κατηγορουμένου και κατ' επέκταση της αρχής της αμεροληψίας, της ανεξαρτησίας και της ισότητας, όπως πηγάζουν από το δικαίωμα στη δίκαιη δίκη του άρθρου 6 ΕΣΔΑ.

Σε αντίθεση με το σχέδιο νόμου, συνυπολογίστηκαν στο τελικό κείμενο οι διατάξεις του ΚΠΔ και συγκεκριμένα του άρθρου 254 και έτσι εισήχθη η ρύθμιση της υποχρεωτικής ειδικής αιτιολογίας στο βούλευμα, το οποίο διατάσσει την άρση του απορρήτου, καθώς και η πρόβλεψη συγκεκριμένων εγγυήσεων για την προστασία του αμέτοχου στο έγκλημα υποκειμένου.

Παρό' όλα αυτά, στο μεγαλύτερο μέρος τους, οι ρυθμίσεις σχετικά με την άρση για την διακρίβωση εγκλημάτων επιδέχονται κριτικής. Στο άρθρο 6 παρ. 10 προβλέπεται η ενημέρωση του θιγόμενου ατόμου σχετικά με την άρση του απορρήτου του για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων από την ΑΔΑΕ, μετά από αίτημά του και με την σύμφωνη γνώμη του του Εισαγγελέα του Αρείου Πάγου και υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε. Η πρώτη προβληματική που διαφαίνεται σε αυτή την διάταξη είναι όμοια με την αντίστοιχη, όσον αφορά στην άρση του απορρήτου για λόγους εθνικής ασφάλειας.

Η άρση τελείται στο πλαίσιο μίας επιχείρησης μυστικής παρακολούθησης για την διακρίβωση ενός εγκλήματος. Πως θα πληροφορηθεί το θιγόμενο άτομο ότι ήταν υποκείμενο της παρακολούθησης αυτής εφόσον αυτή τελείται υπό συνθήκες μυστικότητας; Επιπλέον, καθώς η άρση του απορρήτου αποτελεί μία εξαίρεση από την συνταγματική προστασία του δικαιώματος, καθώς είναι ένα μέτρο με δυσμενείς συνέπειες για τον θιγόμενο, θα έπρεπε το κράτος να τον ενημερώνει και να μην επαφίεται στην δική του πρωτοβουλία, από την στιγμή που δεν προκύψουν, μάλιστα, εις βάρος του στοιχεία ενοχής¹³⁰.

Επιπλέον, στην διάταξη του άρθρου 7 παρ.3 προβλέπεται η συμπερίληψη του υλικού που προέκυψε από την άρση ως αποδεικτικό μέσο για την διαπίστωση διοικητικών παραβάσεων στο πλαίσιο διοικητικής διαδικασίας και ενώπιον των διοικητικών δικαστηρίων. Η εν λόγω ρύθμιση αντιβαίνει στο άρθρο 19 παρ.1,3 Σ. καθώς αυτό προβλέπει ως εξαίρεση από την προστασία του δικαιώματος την άρση του απορρήτου, για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και όχι για την διαπίστωση και περαιτέρω κύρωση διοικητικών παραβάσεων¹³¹.

Τέλος, στο άρθρο 7 παρ. 2 περιλαμβάνονται οι ρυθμίσεις για τα «τυχαία ευρήματα» τα οποία μπορούν να χρησιμοποιηθούν και σε άλλη ποινική δίκη εφόσον το δικαστικό συμβούλιο αποφανθεί ειδικώς περί αυτού για την βεβαίωση ενός εγκλήματος, αλλά δεν υπάρχει σχετική πρόβλεψη για την χρήση τους ως αποδεικτικό υλικό για την υπεράσπιση του κατηγορουμένου σε μία ποινική δίκη.

¹³⁰ (Συμεωνίδου-Καστανίδου, 2022)

¹³¹ (Τσόλιας, 2023)

7.4 Διαδικασία άρσης του απορρήτου

Η διαδικασία άρσης του απορρήτου καθώς και ο διασφαλιστικός ρόλος της ΑΔΑΕ, ως συνταγματικά αρμόδια της τήρησης και του ελέγχου της νομιμότητας ορίζονται στο άρθρο 8 του ν. 5002/2022. Στο εν λόγω άρθρο και συγκεκριμένα στην παράγραφο 2 ορίζεται η διαδικασία αποστολής, λήψης και τήρησης σε ηλεκτρονικό αρχείο, των διατάξεων άρσης και των βουλευμάτων στην Α.Δ.Α.Ε. Σύμφωνα με το εδάφιο δ, «Πρόσβαση στο εν λόγω ειδικό αρχείο καθώς και αναζήτηση στοιχείων πραγματοποιούνται μόνο από τον Πρόεδρο της Α.Δ.Α.Ε. και δύο (2) ακόμη μέλη της Ολομέλειας που ορίζονται από αυτήν. Τα αποτελέσματα της αναζήτησης παρουσιάζονται σε επόμενη συνεδρίαση της Ολομέλειας.».

Οι ειδικότερες ρυθμίσεις για την πρόσβαση στο αρχείο μιας Ανεξάρτητης Αρχής, το οποίο μάλιστα, αποτελεί μια συνήθη λειτουργία για την επιτέλεση των αρμοδιοτήτων της, δεν θα έπρεπε να ορίζεται μια πολύ συγκεκριμένη γραφειοκρατική διαδικασία για την επιτέλεση βασικών λειτουργιών και να ανατίθενται υπαλληλικά καθήκοντα σε μέλη της Ολομέλειας της Αρχής¹³².

Επιπλέον, στην παράγραφο 6, ορίζεται η υποχρεωτική ενημέρωση του Προέδρου της Βουλής, των αρχηγών κομμάτων που εκπροσωπούνται στη Βουλή και του Υπουργού Δικαιοσύνης από τον πρόεδρο της ΑΔΑΕ. Η προβληματική που εγείρεται στο σημείο αυτό αφορά την λειτουργία της ΑΔΑΕ ως συνταγματικά κατοχυρωμένης Ανεξάρτητης Αρχής. Ως μία εκ των πέντε συνταγματικά κατοχυρωμένων Ανεξάρτητων Αρχών, λογοδοτεί ετησίως μόνο στην Επιτροπή Θεσμών και οι αποφάσεις της ως εκτελεστές πράξεις διοικητικών Αρχών, υπόκεινται στον έλεγχο του διοικητικού δικαστή. Το βασικό χαρακτηριστικό τους είναι η ενδοδιοικητική τους ανεξαρτησία, δηλαδή δεν υπάγονται σε ιεραρχικό έλεγχο και οι πράξεις τους δεν υπάγονται σε έλεγχο νομιμότητας. Τα μέλη της ΑΔΑΕ διαθέτουν προσωπική και λειτουργική ανεξαρτησία. Ο σκοπός όλων των παραπάνω είναι να αποφευχθεί η εξάρτηση του έργου των Ανεξάρτητων Αρχών από πολιτικές σκοπιμότητες και γενικότερα η αποφυγή πολιτικών εξαρτήσεων και κάθε μορφή πολιτικής πίεσης εκ μέρους της εκτελεστικής εξουσίας.

Υπό αυτό το πρίσμα, η υποχρέωση ενημέρωσης της ΑΔΑΕ των αρχηγών κομμάτων που εκπροσωπούνται στην Βουλή, καθώς και του Υπουργού Δικαιοσύνης, στον οποίο μάλιστα δεν υπάγεται για ιεραρχικό έλεγχο, αντιβαίνει την εγγύηση ανεξαρτησίας της

¹³²(ΑΔΑΕ Δελτίο Τύπου, 2022)

αποτελεσματικής λειτουργίας της. Η υποχρέωση ενημέρωσης δια νόμου των πολιτικών αρχηγών της Βουλής και του Υπουργού, είναι μία ανάμιξη της εκτελεστικής εξουσίας στο έργο της Α.Δ.Α.Ε, ενώ θα έπρεπε με τον νόμο αυτό να διασφαλίζεται η ανεξάρτητη λειτουργία των Ανεξάρτητων Αρχών.

Ένα από τα σημαντικότερα ελαττώματα του νόμου, εντοπίζεται στην παρ. 4 του άρθρου 8, όπου προβλέπεται η χρονική διάρκεια της παρακολούθησης στους 2 μήνες, με δυνατότητα δίμηνων παρατάσεων, με απώτατο χρονικό όριο τους 10 μήνες. Ωστόσο, αν κριθεί εξαιρετικά πιθανή η διακινδύνευση της εθνικής ασφάλειας, δίνεται η δυνατότητα παράτασης της παρακολούθησης, βάσει συγκεκριμένων στοιχείων, των οποίων η εξακολούθηση της συνδρομής τους επιβεβαιώνεται σε κάθε παράταση της ισχύος της άρσης, χωρίς, όμως, να ορίζεται ένα απώτατο χρονικό διάστημα επέκτασής της. Αυτή η ρύθμιση αντιβαίνει ξεκάθαρα στην νομολογία του ΕΔΔΑ, όπου απαιτεί την θέσπιση ανώτατου χρονικού ορίου παρακολούθησης το οποίο να μην δύναται να ξεπεραστεί, ακόμη κι αν γίνεται η άρση για λόγους εθνικής ασφάλειας.

7.5 Γνωμοδότηση 1/2023 - « Ερμηνεία του Ν. 5002/2022 «Διαδικασία άρσης απορρήτου επικοινωνιών, κυβερνοασφάλεια, προστασία προσωπικών δεδομένων πολιτών»

Η γνωμοδότηση 1/2023¹³³ του τότε Εισαγγελέα του Αρείου Πάγου Ισιδώρου Ντογιάκου παρέχει μια προβληματική ερμηνεία του νόμου 5002/2022 για την άρση του απορρήτου των επικοινωνιών. Η γνωμοδότηση στηρίζει την αφαίρεση της αρμοδιότητας της ΑΔΑΕ να επιληφθεί αιτήματος γνωστοποίησης παρακολούθησης για λόγους εθνικής ασφάλειας, ακόμα και αν υπάρχει καταγγελία για παράβαση της νομιμότητας. Η ερμηνεία αυτή βασίζεται στη θεσμοθέτηση τριμελούς οργάνου που πλέον είναι αρμόδιο για την ενημέρωση, υποβαθμίζοντας τον έλεγχο της ΑΔΑΕ. Ακόμη, κρίνει πως το δικαίωμα ενημέρωσης ενεργοποιείται αποκλειστικά μετά από καταγγελία από τον άμεσα θιγόμενο και περαιτέρω πως αυτό έχει αναδρομική ισχύ και σε παλαιότερες υποθέσεις άρσεως απορρήτου¹³⁴.

¹³³ Γνωμοδότηση 1/2023 Εισαγγελέα Αρείου Πάγου, Διαθέσιμη σε:

<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-1-2023/>

¹³⁴ (Παπασπύρος, 2023) Διαθέσιμο σε: <https://www.constitutionalism.gr/oi-armodiotites-tis-adae-kai-to-kratos-dikaiou/>

Παρά το γεγονός, όμως, πως η ΑΔΑΕ με τον νόμο 5002/2022 στερείται τις παλιές της αρμοδιότητες για έλεγχο στους παρόχους προκειμένου να ενημερώσει τον θιγόμενο για την άρση, δεν στερήθηκε ποτέ τις συνταγματικά κατοχυρωμένες αρμοδιότητές της για έλεγχο τήρησης της νομιμότητας της διαδικασίας των άρσεων του απορρήτου καθώς και της επιβολής κυρώσεων για παραβάσεις αυτών, γεγονός που παραβλέπει η γνωμοδότηση. Οι συγκεκριμένες, δε, αρμοδιότητες είναι αυτοτελείς τόσο προς το νομικό έρεισμα, όσο και προς την λειτουργία σε σχέση με το δικαίωμα ενημέρωσης του θιγόμενου, το οποίο μεταρρυθμίστηκε με τον ν. 5002/2022¹³⁵.

Το πλέον σημαντικό σημείο που πρέπει να σχολιαστεί, σχετικά με την γνωμοδότηση, είναι η προσπάθεια θεμελίωσης της αφαίρεσης αρμοδιοτήτων της ΑΔΑΕ, με τον ισχυρισμό πως ο νόμος 5002/2022 έχει την ισχύ να ανατρέψει και να τροποποιήσει τις αρμοδιότητες της Ανεξάρτητης Αρχής, όπως αυτές εξειδικεύονται στον εκτελεστικό του Συντάγματος νόμο 3115/2003. Οι αρμοδιότητες της ΑΔΑΕ προβλέπονται ρητά στο Σύνταγμα και εξειδικεύονται από τον ν.3115.2003, από τον οποίο αντλεί την νομιμοποίηση να διατελεί ελέγχους και αυτεπαγγέλτως, αλλά και κατόπιν αιτήματος, με σκοπό την διασφάλιση του δικαιώματος του απορρήτου της επικοινωνίας. Μάλιστα, δεν μπορεί να παρακωλυθεί ή να παύσει η ελεγκτική της αρμοδιότητα για λόγους εθνικής ασφαλείας ή να προσκρούσει κατά την διαδικασία άσκησης της ελεγκτικής αρμοδιότητας σε απόρρητο¹³⁶.

Οι αρμοδιότητες αυτές δεν τροποποιήθηκαν με τον ν.5002/2022, οποίος ρύθμισε μόνο ένα καινούριο πλαίσιο, όσον αφορά στην ενημέρωση του θιγόμενου εισάγοντας, κατά παράβαση, μάλιστα, του Συντάγματος και της ευρωπαϊκής νομοθεσίας, ένα πλέγμα απόλυτων περιορισμών¹³⁷. Γιατί, δεν μπορεί να τροποποιηθεί η ελεγκτική αρμοδιότητα της ΑΔΑΕ από τον νομοθέτη, η οποία, της απονέμεται απευθείας από το Σύνταγμα και έχει, όχι απλά δικαίωμα αλλά και υποχρέωση, να ελέγχει τους παρόχους, την ΕΥΠ και όλους τους εμπλεκόμενους φορείς στην διαδικασία άρσης του απορρήτου.

¹³⁵ (Παπασπύρος, 2023)

¹³⁶ (Δήλωση 20 Καθηγητών του Συνταγματικού Δικαίου για την Γνωμοδότηση 1/2023 του Εισαγγελέα του Αρείου Πάγου, 2023), Διαθέσιμο σε: <https://www.constitutionalism.gr/dilosi-20-kathigiton-tou-sintagmatikou-dikaiou-gia-tin-gnomodotisi-1-2023-adae/>

¹³⁷ (Σωτηρέλης, 2023), Διαθέσιμο σε: <https://www.constitutionalism.gr/simtagmatiki-apotimisi-kai-thesmikes-proektaseis-tiw-omothimis-katadikis-tis-gnomodotisis-ntogiakou/>

7.6 Συμπέρασμα κριτικής νόμου

Το νομοθετικό πλαίσιο, όπως περιγράφηκε ανωτέρω μετά την τροποποίηση του ν. 5002/2022 δεν ανταποκρίνεται ούτε στις προδιαγραφές του Συντάγματος, ούτε στις προδιαγραφές της ΕΣΔΑ. Αυτό διαφαίνεται εντονότερα στις ρυθμίσεις, σχετικά με την άρση του απορρήτου, για λόγους εθνικής ασφάλειας. Η συνολική εικόνα που προκύπτει από τις διατάξεις του νόμου είναι, πως η άρση διενεργείται με εισαγγελική διάταξη, χωρίς όμως την απαραίτητη πρόβλεψη αιτιολογίας, ενώ ταυτοχρόνως το δικαίωμα περί γνωστοποίησης στον θιγόμενο δέχτηκε ένα τεράστιο πλήγμα, αφού πια η γνωστοποίηση τελείται τρία χρόνια μετά την παύση ισχύος του μέτρου.

Η γνωστοποίηση θα πραγματοποιείται μετά από αίτημα του ίδιου του θιγόμενου σε τριμελή επιτροπή στην οποία δύο από τα τρία μέλη θα είναι οι εισαγγελικοί λειτουργοί που εξέδωσαν ή ενέκριναν την άρση. Η διάταξη περί σχετικού αιτήματος του θιγόμενου αντιβαίνει την κοινή λογική, καθώς δεν υπάρχει καμία πρόβλεψη για το πως ξαφνικά ένας πολίτης θα λάβει την πρωτοβουλία να απευθυνθεί σε ένα τριμελές όργανο για να ερευνήσει αν έχει γίνει άρση του απορρήτου του για λόγους εθνικής ασφάλειας!

Ταυτοχρόνως, καταλύεται κάθε έννοια ανεξαρτησίας και αμεροληψίας του τριμελούς οργάνου με εξαίρεση την συμμετοχή του τρίτου μέλους, του Προέδρου της Α.Δ.Α.Ε, καθώς συμμετέχουν τα ίδια όργανα που έλαβαν τη απόφαση περί της λήψης του μέτρου με τους εισαγγελικούς λειτουργούς, μάλιστα, να είναι ο ένας άρρηκτα συνδεδεμένος με το περιβάλλον της ΕΥΠ, κατά παράβαση του άρθρου 89 παρ.3 Σ και ο δεύτερος να ορίζεται με απόφαση του (επιλεγμένου από την εκάστοτε κυβέρνηση) Εισαγγελέα του Αρείου Πάγου¹³⁸.

Χωρίς πραγματικό έρεισμα καταλήγει και η διάταξη που θεσπίζει το χρονικό περιθώριο των 3 ετών, το οποίο είναι δυσανάλογο και αυθαίρετο μέτρο και ταυτίζεται με μεγάλο μέρος της διάρκειας της κοινοβουλευτικής περιόδου, ώστε εύκολα συμπεραίνει κανείς πως έτσι αποφεύγεται μεγάλο μέρος της πολιτικής ευθύνης καθώς θα έχει αλλάξει η κοινοβουλευτική σύνθεση άρα και η κυβερνητική θητεία¹³⁹.

¹³⁸ (Χρυσόγονος, 2023) Ανακτήθηκε από: <https://www.constitutionalism.gr/to-arthro-19-tou-sintagmatos-ipo-ti-skia-tou-megalou-adelfou/>

¹³⁹ (Χρυσόγονος, 2023)

Έμφαση πρέπει να δοθεί στο ζήτημα της έλλειψης πρόβλεψης περί υποχρεωτικής αναφοράς των λόγων που στοιχειοθετούν κίνδυνο για την εθνική ασφάλεια. Η αιτιολογία είναι το μέσο, με το οποίο, θα εξεταστεί αν υπάρχει η εξισορρόπηση του επαχθούς μέτρου, που οδηγεί στην παραβίαση της ιδιωτικότητας και της αρχής της αναλογικότητας. Εφαρμόζοντας τα κριτήρια της ευρωπαϊκής νομολογίας, η αιτιολογία αποτελεί την βάση για την διάγνωση του αν το μέτρο ήταν απολύτως αναγκαίο και αν η επέμβαση στον κανονιστικό πυρήνα του δικαιώματος ήταν αναπότρεπτη σε μια δημοκρατική κοινωνία¹⁴⁰. Οι συνέπειες της απουσίας αιτιολογίας είναι αφενός πως δεν μπορεί πρακτικά να πραγματοποιηθεί ο έλεγχος συμβατότητας ενός περιορισμού του δικαιώματος έναντι των γενικών και συνταγματικών αρχών¹⁴¹. Αφετέρου χωρίς αναφορά στην αιτιολογία απουσιάζει και το έρεισμα πάνω στο οποίο θα αναζητήσει ο θιγόμενος αποτελεσματική δικαστική προστασία, κατά παράβαση της νομολογίας του ΕΔΔΑ.

Τέλος, καθίσταται αντισυνταγματικός ο ορισμός της ίδια της έννοιας της εθνικής ασφάλειας στον νόμο 5002/2022 κατ' ερμηνεία του άρθρου 19 παρ. 1Σ, καθώς είναι ευρύς, αόριστος και γενικώς περιλαμβάνοντας οτιδήποτε συναφές με «την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων των Ελλήνων»¹⁴².

Το νομοθετικό πλαίσιο που είχε ως στόχο την ενίσχυση της προστασίας του απορρήτου των επικοινωνιών και τη διαχείριση της άρσης του δεν πέτυχε τους στόχους του. Οι τεχνολογικές εξελίξεις στον τομέα των ηλεκτρονικών επικοινωνιών, που χαρακτηρίστηκαν ως σημαντική βάση, δεν φαίνεται να λήφθηκαν σοβαρά υπόψη.

Αντί να ανανεωθούν οι διατάξεις ώστε να αντικατοπτρίζουν τις σύγχρονες ανάγκες, ο νόμος 5002/2022 διατήρησε σχεδόν αναλλοίωτες τις ρυθμίσεις του νόμου 2225/1994. Ο νομοθέτης επικεντρώθηκε κυρίως σε ζητήματα εθνικής ασφάλειας, αφήνοντας σε δεύτερη μοίρα τη διακρίβωση σοβαρών εγκλημάτων. Ως αποτέλεσμα, η νομοθεσία παρέμεινε ανεπαρκής απέναντι στις προκλήσεις που θέτει η σύγχρονη εποχή.

Ο νέος νόμος απέτυχε να προσαρμοστεί στα κριτήρια που έχει θέσει η ευρωπαϊκή νομολογία του ΕΔΔΑ και του ΔΕΕ για την άρση του απορρήτου, κυρίως, αναφορικά με το

¹⁴⁰ (Παπανικολάου, 2020) Ανακτήθηκε από: <https://www.constitutionalism.gr/wp-content/uploads/2020/07/2020-07-papanikolaou-katerina-aporrto-epikoinonias.pdf>

¹⁴¹ (Παπανικολάου, 2020)

¹⁴² (Χρυσόγονος, 2023)

στοιχείο του «ποιοτικού νόμου» στην εθνική νομοθεσία, ενώ ταυτοχρόνως αγνοήθηκε η επίλυση βασικών δικαιοκρατικών ελλειμμάτων για την εναρμόνιση του νομικού πλαισίου με την συνθήκη της ΕΣΔΑ. Παρ' όλες τις επισημάνσεις της θεωρίας ο νομοθέτης δεν όρισε ρητά το πεδίο εφαρμογής του νόμου, ως τις άρσεις κατά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών που διεξάγονται σε δημόσια δίκτυα και δεν όρισε το περιεχόμενο της έννοιας «πράξη άρσης του απορρήτου». Όσον αφορά το τελευταίο, πράγματι, ο νόμος δεν προσδιορίζει ποιες πράξεις εντάσσονται στην έννοια της άρσης του απορρήτου· αυτό συνάγεται από άλλες διατάξεις, όπως το ΠΔ 47/2005 ή έμμεσα προκύπτει το συμπέρασμα πως άρση του απορρήτου δεν είναι μόνο η συνακρόαση των τηλεφωνικών συνδιαλέξεων, για παράδειγμα, αλλά και η εγγραφή και αποτύπωσή τους σε υλικό φορέα¹⁴³.

Η ραγδαία εξέλιξη της τεχνολογίας των ηλεκτρονικών επικοινωνιών επηρεάζει σημαντικά τα νομικά πλαίσια, ιδίως εντός της ΕΕ. Καθίσταται σαφές, έτσι, ότι οι περιορισμοί του απορρήτου των ηλεκτρονικών επικοινωνιών δεν διέπονται μόνο από την εθνική νομοθεσία, αλλά και από ερμηνείες ευθυγραμμισμένες με την οδηγία 2002/58/ΕΚ. Αυτό καθιστά το δίκαιο της ΕΕ βασική «δίοδο» προς το εθνικό δίκαιο, το οποίο έχει ήδη διαμορφωθεί από την ΕΣΔΑ, διασφαλίζοντας την προστασία των θεμελιωδών δικαιωμάτων μέσω μιας ενιαίας νομικής προσέγγισης. Αυτό διέφυγε στον νομοθέτη σαν παράμετρος, καθώς ο νέος νόμος αντιμετωπίστηκε ως ένα αποκομμένο νομοθέτημα από την ενωσιακή νομοθεσία και από την πραγματικότητα την οποία καλείται να ρυθμίσει.

Η εξελισσόμενη φύση των τεχνολογιών ηλεκτρονικών επικοινωνιών δημιουργεί νέες προκλήσεις στο νομικό πλαίσιο για την προστασία της ιδιωτικής ζωής, σε σχέση και με τα προσωπικά δεδομένα, στον βαθμό που σχετίζεται με την άρση του απορρήτου. Υπάρχουν έννοιες που χρησιμοποιούνται ασαφώς όπως «δημόσια δίκτυα ηλεκτρονικών επικοινωνιών» ή «υπηρεσίες ηλεκτρονικών επικοινωνιών» οι οποίες λαμβάνουν άλλο περιεχόμενο ανάλογα με την πρόοδο της τεχνολογίας, δεδομένου ότι ο σημερινός χρήστης εναλλάσσει τα μέσα και τις μορφές επικοινωνίας ακόμη και μέσα στο εύρος μίας μέρας. Αυτό κατ' επέκταση προϋποθέτει, ότι η νομοθεσία γύρω από την προστασία της ιδιωτικότητας πρέπει να μπορεί να προσαρμοστεί στα δεδομένα αυτά για την αποτελεσματική προστασία του δικαιώματος, γεγονός που δεν επιτυγχάνεται με το νόμο αυτό.

¹⁴³ (Τσόλιας, 2023)

Όσον αφορά την ΑΔΑΕ, ο νόμος 5002/2022 αφαιρέσει αρμοδιότητες που είχε με το προηγούμενο καθεστώς με σημαντικότερη εξ' αυτών την ενημέρωση του θιγόμενου για την άρση του απορρήτου του όταν αυτή είχε διαταχθεί για λόγους εθνικής ασφάλειας και την μετάθεσή της στην τριμελή επιτροπή, γεγονός που διαδραμάτισε σημαντικό ρόλο στην υπόθεση των υποκλοπών, όπως θα φανεί στην συνέχεια.

Γίνεται φανερό πως ο νέος νόμος αποδυνάμωσε το ελεγκτικό έργο της ΑΔΑΕ, στερώντας της την δυνατότητα να απευθύνεται στους παρόχους και να ενημερώνει τους πολίτες για την παραβίαση του δικαιώματός τους για λόγους εθνικής ασφάλειας, προσπαθώντας να γραφειοκρατικοποιήσει την λειτουργία της Ανεξάρτητης Αρχής, αναθέτοντας υπαλληλικά καθήκοντα σε μέλη της και ορίζοντας ένα δυσλειτουργικό πλαίσιο εσωτερικής κατανομής αρμοδιοτήτων. Η ίδια τάση παρατηρείται και στην γνωμοδότηση 1/2023 του τότε Εισαγγελέα του Αρείου Πάγου, όπου επιχειρείται η θεμελίωση της στέρησης αρμοδιοτήτων από την ΑΔΑΕ.

Μετά και τα γεγονότα της υπόθεσης των υποκλοπών, μπορούμε ασφαλώς να καταλήξουμε στο συμπέρασμα ότι οι ανεξάρτητες αρχές βρίσκονται υπό πίεση και ο ρόλος τους αμφισβητείται. Πριν από είκοσι χρόνια, η συνταγματική κατοχύρωση των ανεξάρτητων αρχών επισφράγισε τον ανεξάρτητο ρόλο τους απέναντι στην πολιτική εξουσία. Όμως, σταδιακά μέσω των θεμάτων στελέχωσης των αρχών, την έλλειψη διοικητικής και οικονομικής αυτονομίας, συνεχίζεται η προσπάθεια διάβρωσης της ανεξαρτησίας των Ανεξάρτητων Αρχών¹⁴⁴.

8. Νομολογιακό παράδειγμα στο νέο νομικό πλαίσιο

8.1 Το ιστορικό του «σκανδάλου των υποκλοπών» στην Ελλάδα

Τον Δεκέμβριο του 2021, το Citizen Lab αποκάλυψε την πιθανή χρήση του κατασκοπευτικού λογισμικού Predator στην Ελλάδα, προκαλώντας έντονες ανησυχίες. Η υπόθεση πήρε

¹⁴⁴ (Κοντιάδης, 2023), Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/h-sygtkroysi-anexartitwn-arhwn-kai-politikis-exousias/?fbclid=IwY2xjawFZRvVleHRuA2FlbQIxMQABHcmu2M6w3srIS-GopdCRauvGM_BFexys6Gdfhsxf1Gyg-BOiV1ZWqZeJOW_aem_WA3SbNLMaIwhZsuMzQ8Bw

μεγαλύτερες διαστάσεις τον Ιούλιο του 2022, όταν ο πρόεδρος του ΠΑΣΟΚ-ΚΙΝΑΛ Νίκος Ανδρουλάκης κατήγγειλε ότι το κινητό του είχε μολυνθεί από το κακόβουλο λογισμικό, μετά από ευρήματα της τεχνικής υπηρεσίας του Ευρωπαϊκού Κοινοβουλίου. Επιπλέον, από τον Απρίλιο του ίδιου έτους, δημοσίευμα του Inside Story¹⁴⁵ είχε αναδείξει τη χρήση του Predator για την παρακολούθηση του δημοσιογράφου Θανάση Κουκάκη, εντείνοντας τις ανησυχίες για παραβιάσεις της ιδιωτικότητας.

Τους επόμενους μήνες, συνεχείς δημοσιογραφικές έρευνες αποκάλυψαν, ότι δεκάδες πολίτες είχαν τεθεί υπό παρακολούθηση μέσω του λογισμικού Predator. Τα αρχικά ευρήματα του Citizen Lab επιβεβαιώθηκαν από τεχνικές αναλύσεις της Meta και της Google, ενισχύοντας τις ανησυχίες για την έκταση της παρακολούθησης. Στην αρχή η ελληνική κυβέρνηση αρνήθηκε οποιαδήποτε εμπλοκή των κρατικών αρχών στην αγορά ή χρήση του Predator, παρ' όλο που από τότε η Επιτροπή Pega του Ευρωπαϊκού Κοινοβουλίου εξέφραζε τη βεβαιότητα, ότι το λογισμικό ελέγχεται από την ΕΥΠ ή άλλες οντότητες που δρουν υπό την καθοδήγησή της¹⁴⁶.

Ταυτοχρόνως στις 5 Αυγούστου 2022, μετά από έλεγχο της ΑΔΑΕ, αποκαλύφθηκε ότι η ΕΥΠ είχε προχωρήσει στην άρση του απορρήτου των επικοινωνιών του ευρωβουλευτή και μετέπειτα προέδρου του ΠΑΣΟΚ-ΚΙΝΑΛ, Νίκου Ανδρουλάκη, τον Σεπτέμβριο του 2021. Η παρακολούθηση, που διήρκεσε τρεις μήνες, δικαιολογήθηκε με την επίκληση λόγων εθνικής ασφάλειας. Δεδομένου ότι η άρση απορρήτου ισχύει για δύο μήνες με δυνατότητα παρατάσεων, η ΕΥΠ φαίνεται να ξεκίνησε την παρακολούθηση με αρχική άρση και στη συνέχεια προχώρησε σε επέκτασή της, η οποία ολοκληρώθηκε τον Δεκέμβριο του 2021¹⁴⁷.

Με δήλωσή του ο Πρωθυπουργός ισχυρίστηκε, ότι αγνοούσε την παρακολούθηση του κ. Ανδρουλάκη, αποποιούμενος κάθε πολιτική ευθύνη θεωρώντας ότι αυτή εξαντλήθηκε στην παραίτηση του Διοικητή της ΕΥΠ και του Γενικού Γραμματέα του Πρωθυπουργού¹⁴⁸.

¹⁴⁵ (Τελόγλου, Τριανταφύλλου, 2022) Διαθέσιμο σε: <https://insidestory.gr/article/poios-parakoloythoyse-kinito-toy-dimosiografoy-thanasi-koykaki?token=KVZ0J67X95>

¹⁴⁶ (Μακρής, 2023), Διαθέσιμο σε: https://www.constitutionalism.gr/to-predator-kai-ta-prosopika-dedomena/#_ftn2

¹⁴⁷ (Χονδρόγιαννος, 2022) Διαθέσιμο σε: <https://govwatch.gr/finds/parakoloythisi-toy-nikoy-androylaki-apo-tin-eyp/>

¹⁴⁸ Η από 08/08/2022 δήλωση του Πρωθυπουργού Κυριάκου Μητσοτάκη, Διαθέσιμη σε: <https://www.primeminister.gr/2022/08/08/29961>

Ο Πρωθυπουργός επιχείρησε να αποδώσει την ευθύνη για το σκάνδαλο στους υφιστάμενούς του, παρά το γεγονός, ότι σύμφωνα με την επικρατούσα συνταγματική ερμηνεία, η «αντικειμενική» ευθύνη βαρύνει τον ίδιο, καθώς είναι ο πολιτικός και διοικητικός προϊστάμενος των υπηρεσιών αυτών. Η ευθύνη που καταλογίστηκε περιορίστηκε σε «λάθη» και «ανεπαρκείς» ή «μη αποδεκτούς πολιτικά χειρισμούς», χωρίς να γίνεται λόγος για «συνειδητή παραπλάνηση» του Κοινοβουλίου σε θέματα αρμοδιότητάς του.

Την περίοδο του φθινοπώρου του 2022, η εφημερίδα *Documento* δημοσίευσε πληροφορίες που υποστήριζαν ότι μια σειρά δημόσιων προσώπων ήταν υπό παρακολούθηση από την ΕΥΠ. Μετά από αιτήματα δύο προσώπων, του ευρωβουλευτή Γιώργου Κύρτσου και του δημοσιογράφου Τάσου Τέλλογλου, η ΑΔΑΕ προχώρησε σε σχετικούς ελέγχους, οι οποίοι κατέδειξαν ότι αμφότεροι παρακολουθούνταν από την ΕΥΠ. Στη συνέχεια, μετά από αίτημα του τότε αρχηγού της αξιωματικής αντιπολίτευσης, Αλέξη Τσίπρα, στην ΑΔΑΕ, αποκαλύφθηκε τον Ιανουάριο του 2023 από τον Πρόεδρο της ΑΔΑΕ, Χρήστο Ράμμο, ότι παρακολουθούνταν για μήνες από την ΕΥΠ και άλλα άτομα μεταξύ των οποίων και ένας Υπουργός της Κυβέρνησης και ο αρχηγός των Ενόπλων Δυνάμεων.

Τον Μάιο του 2023, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε την τελική έκθεση της επιτροπής PEGA, η οποία ερευνούσε τη χρήση κατασκοπευτικών λογισμικών. Η έκθεση κατέληξε στο συμπέρασμα ότι το λογισμικό αυτό είχε αξιοποιηθεί από την ανώτατη πολιτική ηγεσία της Ελλάδας.

Τον Σεπτέμβριο του 2023, η Διάσκεψη των Προέδρων της Βουλής προχώρησε στην αντικατάσταση των μελών της ΑΔΑΕ, μόλις μία ημέρα πριν την προγραμματισμένη συνεδρίαση της Αρχής, για να επιβάλει πρόστιμο στην ΕΥΠ λόγω της μη ικανοποιητικής συνεργασίας της στην έρευνα. Στη συνέχεια, η νέα σύνθεση της ΑΔΑΕ απέρριψε το αίτημα των δύο εισαγγελέων, που ερευνούσαν την υπόθεση από το 2022, να εξετάσει εάν τα 92 άτομα, που είχαν εντοπιστεί από την Αρχή Προστασίας Δεδομένων ως στόχοι του λογισμικού Predator, παρακολουθούνταν επίσης από την ΕΥΠ.

Τον Σεπτέμβριο του 2022 ο κος Ανδρουλάκης με αίτημά του στην ΑΔΑΕ είχε ζητήσει να του γνωστοποιηθούν η εισαγγελική διάταξη και ο πλήρης φάκελος με το υλικό που είχε συλλεγεί, μετά την επιβολή σε βάρος του, του μέτρου άρσης του απορρήτου των

επικοινωνιών του, αλλά μετά από πράξη της Αρχής, το αίτημα είχε απορριφθεί βάσει των ισχυόντων διατάξεων του νόμου 5002/2022 σχετικά με την γνωστοποίηση του μέτρου.

Ο πρόεδρος του ΠΑΣΟΚ-KΙΝΑΛ προσέφυγε τον Νοέμβριο του 2022, ενώπιον της Ολομέλειας του ΣτΕ ζητώντας να κριθεί ως αντισυνταγματική και μη εναρμονισμένη με την ΕΣΔΑ, τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε. καθώς και την Οδηγία 2002/58, η διάταξη της τροπολογίας του 2021 που δεν επιτρέπει στην ΑΔΑΕ να ενημερώνει του θιγόμενους από την παραβίαση της ιδιωτικότητάς τους όταν επρόκειτο για άρση του απορρήτου για λόγους εθνικής ασφάλειας. Στρέφεται, επίσης, κατά της ΑΔΑΕ, όπου με απόφασή της αρνήθηκε να τον ενημερώσει εφαρμόζοντας τον νόμο 5002/2022.

Επί της αίτησης αυτής το ΣτΕ εξέδωσε την απόφαση 465/2024 με την οποία ομόφωνα έκρινε αντισυνταγματική την τροπολογία του 2021, η οποία καταργούσε τη δυνατότητα των παρακολουθούμενων να ζητήσουν να ενημερωθούν για τον λόγο και τον χρόνο της παρακολούθησής τους και έκρινε ότι εφαρμόζεται στην υπόθεση Ανδρουλάκη η προϊσχύουσα ρύθμιση του νόμου 2225/1994. Σύμφωνα με αυτήν, μετά τη λήξη του μέτρου της άρσης και υπό την αναγκαία προϋπόθεση ότι δεν διακινδυνεύεται ο σκοπός για τον οποίο διατάχθηκε, μπορεί η ΑΔΑΕ να αποφασίζει τη γνωστοποίηση της επιβολής του στους θιγόμενους¹⁴⁹.

Στις 24 Απριλίου η ΑΔΑΕ με δελτίο τύπου που εξέδωσε ανακοίνωσε την απόφαση της Ολομέλειας της ΑΔΑΕ να συμμορφωθεί με την απόφαση 465/2024 ΣτΕ¹⁵⁰. Η ΑΔΑΕ στην συνέχεια συμμορφούμενη με την απόφαση του ΣτΕ απηύθυνε αίτημα στην διοίκηση της ΕΥΠ. καθώς και στον εποπτεύοντα εισαγγελέα, ζητώντας να ενημερωθεί για το περιεχόμενο του φακέλου της άρσης απορρήτου του Νίκου Ανδρουλάκη.

Στις 8 Μαΐου 2024 ο εποπτεύων εισαγγελέας της υπηρεσίας απάντησε πως οι εκάστοτε εποπτεύοντες εισαγγελείς δεν τηρούν φακέλους υποθέσεων και ως εκ τούτου ο ίδιος δεν έχει πρόσβαση στον φάκελο της παρακολούθησης του προέδρου του ΠΑΣΟΚ-KΙΝΑΛ

¹⁴⁹ (Κοντιάδης, 2024) Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/h-apofasi-androulaki-tou-ste/?fbclid=IwZXh0bgNhZW0CMTEAAR0CaIJ4HWnZNa7T8Y6RDPULbAe6yxmdl6C1dWjWgwR4yGv7gh3Dzbj0EOs_aem_rJrWf7P-4Nre9oDt2A84jg

¹⁵⁰ Δελτίο Τύπου-Απόφαση της ΑΔΑΕ, 24/04/2024, Διαθέσιμο σε: <https://adae.gov.gr/enimerosi/deltiotypou/deltio-tyπου-apophase-tes-adae>

Νίκου Ανδρουλάκη¹⁵¹. Η διοίκηση της ΕΥΠ αρνήθηκε να παράσχει τις πληροφορίες σχετικά με το περιεχόμενο του φακέλου, όπως είχε ζητηθεί.

Τον Ιούνιο του 2024 η ΑΔΑΕ συνεδρίασε προκειμένου να αποφασιστεί αν θα κληθεί ο διοικητής της ΕΥΠ να παράσχει εξηγήσεις σχετικά με την άρνηση της ΕΥΠ να ενημερώσει για τους λόγους παρακολούθησης του Νίκου Ανδρουλάκη. Με οριακή ψηφοφορία (4-3) αποφασίστηκε να μην κληθεί ο διοικητής της ΕΥΠ σε ακρόαση ενώπιον της ΑΔΑΕ¹⁵². Τον Ιούλιο 2024 ο κος Ανδρουλάκης προσέφυγε εκ νέου στο Ευρωπαϊκό Δικαστήριο¹⁵³, μετά την άρνηση της ΕΥΠ να συμμορφωθεί με την απόφαση του ΣτΕ και να κοινοποιήσει στην ΑΔΑΕ τους λόγους για τους οποίους διατάχθηκε το μέτρο της άρσης του απορρήτου του.

Στις 30 Ιουλίου 2024, η Εισαγγελέας του Αρείου Πάγου, Γεωργία Αδειλίνη, ανακοίνωσε¹⁵⁴ την ολοκλήρωση της προκαταρκτικής εξέτασης για την υπόθεση των υποκλοπών και την θέση της υπόθεσης στο αρχείο όσον αφορά στην ΕΥΠ και άλλες κρατικές υπηρεσίες, όπως την Ελληνική Αστυνομία και την Αντιτρομοκρατική. Παράλληλα, «δεν υπήρξε καμία απολύτως εμπλοκή με το κατασκοπευτικό λογισμικό predator ή οποιοδήποτε άλλο παρόμοιο λογισμικό κρατικής υπηρεσίας και δη της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ), της Αντιτρομοκρατικής (Δ.Α.Ε.Ε.Β.) και γενικότερα της ΕΛΑΣ (Υπουργείο Προστασίας του Πολίτη) ή οποιοδήποτε κρατικού λειτουργού».

Ανακοίνωσε ποινικές διώξεις εναντίον τεσσάρων ατόμων, που ήταν εκπρόσωποι και ιδιοκτήτες εταιρειών συνδεδεμένων με τη χρήση του λογισμικού Predator στην Ελλάδα. Παράλληλα, η πειθαρχική έρευνα για την εισαγγελέα που επέβλεπε την ΕΥΠ

¹⁵¹ (Σουλιώτης, 2024), Διαθέσιμο σε: <https://www.kathimerini.gr/society/563026948/yprothesi-androylaki-apantisi-eyp-stin-adae-choris-dieykriniseis/>

¹⁵² Efsyn, Υποκλοπές: Η ΑΔΑΕ δεν καλεί σε ακρόαση την ΕΥΠ για την παρακολούθηση Ανδρουλάκη, 2024, Διαθέσιμο σε: https://www.efsyn.gr/politiki/kybernisi/435583_ypoklopes-i-adae-den-kalei-se-akroasi-tin-eyp-gia-tin-parakoloythisi

¹⁵³ Η ΑΥΓΗ, **Ανδρουλάκης για υποκλοπές** / Προσέφυγε ξανά στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, 26-07-2024, Διαθέσιμο σε: https://www.avgi.gr/politiki/490889_prosefyge-xana-sto-eyropaiko-dikastirio-anthropinon-dikaiomaton?fbclid=IwZXh0bgNhZW0CMTEAAR2K2ntzhdE3qworGv7cAsZ_jfLB-e0TkbDcHvTWjpghwIjGNkDF9EIjuemM_aem_VhpdMSJFetdALY3_WO6pIA

¹⁵⁴ Εισαγγελία Αρείου Πάγου, **Ανακοίνωση – Ενημέρωση σχετικά με τις υποκλοπές 30.7.2024**, Διαθέσιμο σε: <https://eisap.gr/%CE%B1%CE%BD%CE%B1%CE%BA%CE%BF%CE%AF%CE%BD%CF%89%CF%83%CE%B7-30-7-2024/>

αρχαιοθετήθηκε, ενώ ο Άρειος Πάγος και η Εισαγγελία αρνήθηκαν να δώσουν τα στοιχεία στη Βουλή, επικαλούμενοι την ανεξαρτησία της δικαιοσύνης. Σύμφωνα με την ανακοίνωση της Εισαγγελέως του Αρείου Πάγου «Ως προς δε τις διατάξεις περί άρσης απορρήτου των επικοινωνιών, που εκδόθηκαν από την τότε Εισαγγελέα της ΕΥΠ και αφορούν τα έτη 2020-2024, τηρήθηκε απαρέγκλιτα η διαδικασία που προβλέπεται από το Νόμο, ο οποίος, εκτός των άλλων, διαχρονικά, δεν αξιώνει την παράθεση ειδικής αιτιολογίας στις ως άνω διατάξεις, η σχετική δε πρόβλεψη, η οποία θεσμοθετήθηκε το πρώτον με το Ν. 2225/1994, διατηρήθηκε συνεχώς από όλες τις Κυβερνήσεις μέχρι τον νέο Ν. 5002/9-12-2022».

Η ανακοίνωση αυτή δημιούργησε μεγάλη πολιτική ένταση και τον Αύγουστο του 2024 τα κόμματα της αντιπολίτευσης στην Βουλή κατέθεσαν αίτημα προς ψήφιση ώστε να διαβιβαστούν το πόρισμα και η πράξη αρχειοθέτησης της Εισαγγελίας του Αρείου Πάγου και να κληθούν η Εισαγγελέας και ο Αντιεισισαγγελέας του Αρείου Πάγου, που διενήργησαν την προκαταρκτική έρευνα στην Επιτροπή Θεσμών και Διαφάνειας προς ενημέρωση, το οποίο καταψηφίστηκε.

8.2 Απόφαση 465/2024 ΣτΕ

Με την απόφαση 465/2024¹⁵⁵, η Ολομέλεια του Συμβουλίου της Επικρατείας έκανε δεκτή εν μέρει την αίτηση ακύρωσης κατά πράξης του Προέδρου της ΑΔΑΕ. Η πράξη αυτή αφορούσε την απόρριψη αιτήματος του αιτούντος, πρώην ευρωβουλευτή και αρχηγού του ΠΑΣΟΚ – ΚΙΝΑΛ, που είχε υποβληθεί στις 7 Σεπτεμβρίου 2022. Ο αιτών ζητούσε να του κοινοποιηθούν η εισαγγελική διάταξη και το σύνολο του φακέλου με το υλικό που είχε συγκεντρωθεί σχετικά με την άρση του απορρήτου των επικοινωνιών του, σύμφωνα με συγκεκριμένες διατάξεις του νόμου 2225/1994 (άρθρο 5 παρ. 4, 9). Η απόφαση αυτή αποτελεί την πρώτη παρέμβαση ανώτερης δικαστικής αρχής σχετικά με το ζήτημα των υποκλοπών και έχει ιδιαίτερα μεγάλη σημασία λόγω των νομικών της συμπερασμάτων.

8.2.1. Δικαίωμα γνωστοποίησης

Σχετικά με το δικαίωμα γνωστοποίησης, στο προηγούμενο νομικό καθεστώς και τον νόμο 2225/1994 υπήρξε τροποποίηση των διατάξεων περί «γνωστοποίησης» στο θιγόμενο πρόσωπο της επιβολής εις βάρος του, του μέτρου της άρσης του απορρήτου, με την διάταξη του άρθρου 87 του ν. 4790/2021, σύμφωνα με την οποία εξαιρέθηκε η δυνατότητα

¹⁵⁵ 465/2024 ΣτΕ, Διαθέσιμη [εδώ](#).

ενημέρωσης των θιγόμενων για την άρση του απόρρητου των επικοινωνιών τους, όταν η άρση επιβλήθηκε για λόγους «εθνικής ασφάλειας».

Στο προϊσχύσαν νομικό πλαίσιο σύμφωνα με το άρθρο 5 παρ. 9, η γνωστοποίηση στον θιγόμενο πραγματοποιούνταν από την ΑΔΑΕ πληρουμένων των απαραίτητων όρων της άρσης του μέτρου, της μη διακινδύνευσης του σκοπού για τον οποίο είχε διαταχθεί εξαρχής και της σύμφωνης γνώμης του Εισαγγελέα του Αρείου Πάγου. Επομένως, αυτό που εισήγαγε ο ν. 4990/2021 στο άρθρο 87 ήταν μία **γενική και απόλυτη εξαίρεση** από το δικαίωμα γνωστοποίησης στον θιγόμενο με μόνη βάση την επίκληση λόγων «εθνικής ασφάλειας»¹⁵⁶. Η ρύθμιση κατατέθηκε τον Μάρτιο του 2021, με εκπρόθεσμη τροπολογία σε πολυνομοσχέδιο του υπουργείου Υγείας, ενώ είχε ήδη αποκαλυφθεί η παρακολούθηση του δημοσιογράφου Θανάση Κουκάκη, ο οποίος από τον Αύγουστο του 2020 ζητούσε ενημέρωση για την άρση του απόρρητου των επικοινωνιών του. Η ρύθμιση απαγόρευσε αναδρομικά στην ΑΔΑΕ να ενημερώνει όσους παρακολουθούνταν για λόγους εθνικής ασφάλειας¹⁵⁷.

Σύμφωνα με το ΣτΕ η διάταξη του άρθρου 87 του ν. 4790/2021¹⁵⁸, που απαγορεύει πλήρως την ενημέρωση του προσώπου του οποίου το απόρρητο επικοινωνιών άρθηκε για λόγους εθνικής ασφάλειας, ακόμα και μετά τη λήξη του μέτρου και χωρίς να έχει προκύψει κίνδυνος για την εθνική ασφάλεια, πρόκειται για υπέρμετρο περιορισμό του απαραβίαστου της επικοινωνίας. Αυτός ο περιορισμός δεν δικαιολογείται στο πλαίσιο του κράτους δικαίου και αντίκειται στο Σύνταγμα, στην οδηγία 2002/58, στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και στην ΕΣΔΑ, καθιστώντας τη διάταξη ανίσχυρη¹⁵⁹.

Συγκεκριμένα, οι παραβιάσεις του ελληνικού Συντάγματος, από την τροπολογία του ν. 4990/2021, θεμελιώνονται στη μη τήρηση των προϋποθέσεων άρσης του δικαιώματος γνωστοποίησης, που συνδέεται άμεσα με το απόρρητο των επικοινωνιών. Οι παραβιάσεις του ειδικού ελληνικού νόμου προκύπτουν από τον γενικό και απόλυτο χαρακτήρα της απαγόρευσης ενημέρωσης. Τέλος, οι παραβιάσεις του κοινοτικού δικαίου οφείλονται στη

¹⁵⁶ (Μποτόπουλος, 2024)

¹⁵⁷ (Κρουστάλλη, 2024)

¹⁵⁸ (Ράμμος Χ., Γκριτζαλης Σ. & Παπανικολάου Α., 2021), Διαθέσιμο σε:

https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/#_ftnref1

¹⁵⁹ 465/2024 ΣτΕ

μη συμμόρφωση της εθνικής νομοθεσίας με τους κανόνες και τα όρια που θέτει η ΕΕ για την προστασία των προσωπικών δεδομένων¹⁶⁰.

Το δικαστήριο προχώρησε περαιτέρω, καθορίζοντας ότι η ενημέρωση του θιγόμενου πρέπει να περιλαμβάνει το αιτιολογικό της άρσης του απορρήτου των επικοινωνιών, ώστε να διασφαλίζεται η δυνατότητα αποτελεσματικής δικαστικής προστασίας. Αυτή η διευκρίνιση υποδηλώνει ότι η αιτιολόγηση πρέπει να είναι συγκεκριμένη, επιτρέποντας κατ' αυτόν τον τρόπο, τον ουσιαστικό δικαστικό έλεγχο της νομιμότητας της παρακολούθησης.

Η λήξη ενός μέτρου άρσης του απορρήτου των επικοινωνιών ενός ατόμου και η απουσία λόγων που να καθιστούν πλέον αναγκαία τη διατήρηση της μυστικότητάς του, εγείρουν το κρίσιμο ζήτημα της εκ των υστέρων ενημέρωσης του θιγόμενου προσώπου. Η παράλειψη γνωστοποίησης στον πολίτη της επιβολής του μέτρου παρακολούθησης στερεί από αυτόν τη δυνατότητα να προσβάλει τη νομιμότητα της εν λόγω ενέργειας. Υπό αυτές τις συνθήκες, η παρακολούθηση, από μια διοικητική πράξη που υπόκειται σε έλεγχο νομιμότητας, υποβαθμίζεται σε απλή υλική ενέργεια, για την οποία το θιγόμενο άτομο αδυνατεί να ασκήσει ένδικα βοηθήματα. Η ενημέρωση αυτή συνιστά ουσιώδες προαπαιτούμενο για την άσκηση των δικαιωμάτων του ατόμου, καθώς του παρέχει τη δυνατότητα να προσφύγει στη δικαιοσύνη, εφόσον θεωρήσει ότι το μέτρο εφαρμόστηκε κατά τρόπο μη σύννομο, καταχρηστικό ή δυσανάλογο, προκαλώντας έτσι παραβίαση του δικαιώματός του στην προστασία της ιδιωτικής του ζωής.

Αν, αντίθετα, δεν προβλέπεται η υποχρέωση γνωστοποίησης ή αυτή απαγορεύεται, το άτομο ενδέχεται να μην πληροφορηθεί ποτέ ότι υπήρξε αντικείμενο παρακολούθησης. Μια τέτοια κατάσταση οδηγεί αναπόφευκτα στον αποκλεισμό του από την άσκηση ένδικων βοηθημάτων και μέσων, στερώντας του την πρόσβαση σε αποτελεσματική δικαστική προστασία. Επομένως, πλήττεται άμεσα η πραγμάτωση των δικαιωμάτων του ατόμου και εδραιώνεται ένα καθεστώς αδιαφάνειας.

8.2.3 Ο όρος «εθνική ασφάλεια» και η επέμβασή του στο δικαίωμα

Το ΣτΕ στην απόφασή του θέτει ως κεντρικό ζήτημα την έννοια της «εθνικής ασφάλειας» και τον τρόπο με τον οποίο αυτή μπορεί να χρησιμοποιηθεί ως αιτία για τον περιορισμό του απορρήτου των επικοινωνιών, που κατοχυρώνεται στο άρθρο 19 παρ. 1 του

¹⁶⁰ (Μποτόπουλος, 2024)

Συντάγματος. Αν και το Σύνταγμα και οι σχετικοί νόμοι, καθώς και η Ενωσιακή νομοθεσία, προβλέπουν τη δυνατότητα άρσης του απορρήτου για λόγους εθνικής ασφάλειας, το ΣτΕ υπογραμμίζει ότι αυτή η άρση δεν μπορεί να είναι απόλυτη, ούτε να οδηγεί σε μόνιμο αποκλεισμό δικαιωμάτων, όπως το δικαίωμα ενημέρωσης του ατόμου για την παρακολούθηση των επικοινωνιών του.

Το δικαστήριο επισημαίνει, ότι η άρση του απορρήτου πρέπει να είναι προσωρινή και να περιορίζεται σε περιπτώσεις όπου εξακολουθεί να υπάρχει απειλή για την εθνική ασφάλεια. Μόλις η απειλή αυτή πάψει να υφίσταται ή διαπιστωθεί, ότι δεν υπήρξε ποτέ, πρέπει να επανέλθει η «κανονικότητα», δηλαδή η προστασία του απορρήτου και η ενημέρωση του θιγόμενου προσώπου. Επισημαίνει, ακόμη, πρέπει να αποφεύγεται μια απόλυτη και χωρίς όρια άρση του απορρήτου, καθώς συνιστά παραβίαση των συνταγματικών και ενωσιακών αρχών της αναλογικότητας.

Η απόφαση τονίζει ότι η εθνική ασφάλεια δεν μπορεί να χρησιμοποιείται ως γενικός και απόλυτος λόγος για την παραβίαση θεμελιωδών δικαιωμάτων, δίνοντας έμφαση στο στοιχείο της προσωρινότητας και του εκτάκτου ενός τέτοιου μέτρου. Στο πλαίσιο μιας δημοκρατικής κοινωνίας, όπως προβλέπεται τόσο από το Σύνταγμα όσο και από την ευρωπαϊκή νομοθεσία, η χρήση του όρου «εθνική ασφάλεια» πρέπει να υπόκειται σε περιορισμούς και να μην γίνεται προσχηματική. Η απολυτότητα της εξαίρεσης της «εθνικής ασφάλειας», η αυτονόμησή της και η επίκλησή της ως γενικός λόγος αποκλεισμού για την άσκηση ενός θεμελιώδους δικαιώματος δεν είναι συμβατή με το Σύνταγμα¹⁶¹. Η άρση του απορρήτου των επικοινωνιών πρέπει να παραμένει εξαίρεση και όχι κανόνας, διασφαλίζοντας ότι τα θεμελιώδη δικαιώματα προστατεύονται σε κάθε περίπτωση.

8.2.3. Συμμόρφωση της Διοίκησης και χρονική ισχύς νόμου

Η απόφαση του ΣτΕ παρέχει διευκρινίσεις σχετικά με δύο κρίσιμα ζητήματα. Πρώτον, αναφέρεται στην υποχρέωση της Διοίκησης να συμμορφώνεται με τις μεταβολές στο νομοθετικό καθεστώς μετά την άσκηση μιας αίτησης ακύρωσης. Η Διοίκηση καλείται να εκδίδει νέα διοικητική πράξη, βασισμένη στο νομικό και πραγματικό καθεστώς που ίσχυε κατά τον χρόνο της ακυρωθείσας πράξης, εκτός αν ο νομοθέτης έχει θεσπίσει μεταγενέστερες διατάξεις με αναδρομική ισχύ. Δεύτερον, η απόφαση διευκρινίζει την

¹⁶¹ (Μποτόπουλος, 2024)

έννοια της λυσιτέλειας, δηλαδή ότι η ακύρωση μιας πράξης είναι λυσιτελής μόνο όταν επιφέρει ουσιαστικό όφελος στον αιτούντα, διορθώνοντας τη βλάβη που υπέστη στα έννομα συμφέροντά του¹⁶².

Ιδιαίτερα ενδιαφέρουσα είναι η ερμηνεία που δίνει το ΣτΕ σχετικά με την εφαρμογή των νομοθετικών αλλαγών στον ν. 2225/1994 και στον μεταγενέστερο ν. 5002/2022. Η απόφαση επισημαίνει ότι οι τροποποιήσεις αυτές δεν αναιρούν τη λυσιτέλεια της αίτησης ακύρωσης, καθώς οι διατάξεις του ν. 5002/2022 δεν έχουν αναδρομική ισχύ και δεν επηρεάζουν εκκρεμή αιτήματα γνωστοποίησης άρσης απορρήτου που υποβλήθηκαν πριν από την εφαρμογή του νέου πλαισίου. Αυτό διασφαλίζει ότι η αίτηση ακύρωσης εξακολουθεί να έχει ουσιαστικό και δικονομικό ενδιαφέρον και πρέπει να εξεταστεί από τη Διοίκηση.

Το ΣτΕ, παρά την ύπαρξη του νεότερου νομοθετικού πλαισίου, επιλέγει να χρησιμοποιήσει τη διάταξη της παρ. 9 του άρθρου 5 του ν. 2225/1994, όπως ίσχυε πριν από την ακυρωθείσα διάταξη του ν. 4790/2021, αντί του ν. 5002/2022. Ο λόγος είναι ότι ο ν. 5002/2022 αφορά μόνο μελλοντικά αιτήματα και δεν μπορεί να εφαρμοστεί σε εκκρεμείς υποθέσεις που υπάγονται στο προγενέστερο νομοθετικό καθεστώς. Η απόφαση επιστρέφει στο προηγούμενο σύστημα ενημέρωσης, όπου η γνωστοποίηση προς τον θιγόμενο γίνεται μέσω της Ολομέλειας της ΑΔΑΕ, ενώ το νέο σύστημα προβλέπει πιο περιοριστικούς όρους, όπως την πάροδο τριετίας και την κρίση ειδικής τριμελούς επιτροπής.

Ωστόσο, η επιλογή του ΣτΕ να αναβιώσει τη διάταξη του ν. 2225/1994, η οποία είχε καταργηθεί ρητά με τον ν. 5002/2022 είναι άξια επισήμανσης. Παρά την κατάργηση της διάταξης, το ΣτΕ προκρίνει την εφαρμογή της για την εξυπηρέτηση της προστασίας των δικαιωμάτων των πολιτών, επισημαίνοντας ότι ο σκοπός της ενημέρωσης του θιγόμενου πρέπει να υπερισχύσει. Αυτή η προσέγγιση είναι ένα θετικό και τολμηρό βήμα, καθώς η απόφαση βασίζεται σε μια διάταξη που τυπικά δεν ισχύει πλέον, αλλά επανέρχεται για λόγους ουσιαστικής προστασίας δικαιωμάτων.

Με την απόφαση 465/2024, το ΣτΕ καταδικάζει τη νομοθετική παρέμβαση που εισήγαγε γενική απαγόρευση ενημέρωσης για την άρση του απορρήτου των επικοινωνιών, κρίνοντας την διάταξη αντισυνταγματική. Πήρε θέση τόσο για τον τρόπο που νομοθέτησε η Κυβέρνηση την εξαίρεση αυτή όσο και για την ουσία της ρύθμισης που παραβιάζει

¹⁶² (Πρεβεδούρου, 2024)

θεμελιώδη δικαιώματα, χρησιμοποιώντας εκπρόθεσμη τροπολογία σε άσχετο νομοσχέδιο για την πανδημία και την προστασία της δημόσιας υγείας, σε ένα χρονικό διάστημα κατά το οποίο είχε ήδη ξεκινήσει η υπόθεση των υποκλοπών. Η απόφαση υπογραμμίζει ότι το νέο νομοθετικό πλαίσιο του ν. 5002/2022 δεν διόρθωσε την παραβίαση του κράτους δικαίου κατά τον χειρισμό των άρσεων απορρήτου στην υπόθεση των υποκλοπών, καθώς ο ίδιος ο νόμος συνεχίζει να περιορίζει τα ατομικά δικαιώματα χωρίς επαρκή προστασία. Η κυβέρνηση, κατά το ΣτΕ, επέδειξε δυσανεξία στη διαφάνεια και τη λογοδοσία, κάτι που αντιβαίνει στις αρχές του κράτους δικαίου, καθιστώντας τις πρακτικές της αμφισβητήσιμες και ασύμβατες με την προστασία των θεμελιωδών δικαιωμάτων των πολιτών¹⁶³.

Συμπέρασμα

Σε μια ολοένα μεταβαλλόμενη πραγματικότητα, όπου οι ψηφιακές αλλαγές είναι κατακλυσμιαίες, είναι αναπόφευκτο να μην μείνει ανεπηρέαστο το πεδίο της επικοινωνίας. Τα μεταδεδομένα επικοινωνίας είναι άμεσα συνδεδεμένα με την μαζική επιτήρηση, μέσω των μεθόδων γενικής διατήρησης μεταδεδομένων και των άρσεων των απορρήτων από τις αρχές, επιτελώντας κρίσιμο ρόλο, λόγω της ικανότητας σκιαγράφησης βιοπροφίλ των επικοινωνούντων και της αποκάλυψης ευαίσθητων πληροφοριών για τα άτομα.

Η ενωσιακή νομολογία γύρω από τη μαζική παρακολούθηση έχει πλέον διαμορφώσει ένα πλαίσιο, όπου τέτοιες πρακτικές επιτρέπονται, υπό την προϋπόθεση ότι συνοδεύονται από συγκεκριμένες εγγυήσεις για την αποτροπή καταχρήσεων, οι οποίες στην πράξη μετατρέπονται σε συμβολικές διαδικασίες εποπτείας. Τόσο το ΔΕΕ όσο και το ΕΔΔΑ έχουν παρουσιάσει μία αυξημένη τάση αναγνώρισης των συστημάτων μαζικής παρακολούθησης για λόγους «εθνικής ασφάλειας», με πρόσχημα τυπικές, διαδικαστικές, δικλείδες ασφαλείας. Ωστόσο, η εφαρμογή αυτών των προτύπων αφήνει σημαντικά περιθώρια ευελιξίας στα κράτη μέλη και στις μυστικές υπηρεσίες, ιδιαίτερα όσον αφορά ζητήματα που άπτονται της «εθνικής ασφάλειας», επιτρέποντας ακόμη και την γενική διατήρηση μεταδεδομένων, βάσει απειλών για την «εθνική ασφάλεια». Η δικαστική εξουσία στην Ευρώπη απεκδύεται του εποπτικού ρόλου της τήρησης και της προστασίας του θεμελιώδους δικαιώματος στο απόρρητο των επικοινωνιών και προσφέρει την «εθνική

¹⁶³ (Μποτόπουλος, 2024)

ασφάλεια» ως λευκό χαρτί στα κράτη-μέλη, πάνω στο οποίο σχεδιάζονται τα συστήματα μαζικής παρακολούθησης.

Σε αυτή την πραγματικότητα ρυθμίστηκε και το ελληνικό νομικό πλαίσιο με τον νόμο 5002/2022, ο οποίος δεν τηρεί σε μεγάλο ποσοστό, ούτε τις τυπικές εγγυήσεις που επιζητεί η ενωσιακή νομοθεσία. Παρ' ότι, για πρώτη φορά, αναγνωρίστηκε ρητά σε εκτελεστικό νόμο και έφυγε από την σφαίρα της θεωρίας, η ισότιμη προστασία των μεταδεδομένων της επικοινωνίας με το περιεχόμενο αυτής, πλείστες άλλες διατάξεις επιτρέπουν την καταστρατήγηση του απορρήτου των επικοινωνιών. Χαρακτηριστικό παράδειγμα είναι η άρση απορρήτου για λόγους «εθνικής ασφάλειας», όπου αποτελεί και στον ελληνικό νόμο μία ρύθμιση αόριστη, χωρίς επαρκείς εγγυήσεις (έλλειψη αιτιολογίας, έλλειψη αναφοράς ονοματεπώνυμου στη διάταξη άρσης, καθυστέρηση ενημέρωσης και συνεπώς καθυστέρηση ένδικης προστασίας του θιγόμενου και αδυναμία ενημέρωσης λόγω πρόβλεψης πρωθύστερου αιτήματος του θιγόμενου κ.α). Η «εθνική ασφάλεια», επομένως, γίνεται μία ρύθμιση πασπαρτού, όπου μπορεί να αποτελέσει εργαλείο για την κατάχρηση της εξουσίας άρσης του απορρήτου, με την τήρηση κάποιων τυπικών, αλλά όχι ουσιαστικών εγγυήσεων.

Η έλλειψη των θεσμικών εγγυήσεων στο ελληνικό νομικό πλαίσιο, καθρεφτίστηκε στην «υπόθεση των υποκλοπών». Μέσα από αυτή αναδείχθηκε η κρίση την οποία βιώνει το κράτος δικαίου στην Ελλάδα, ως προς την προστασία των θεμελιωδών δικαιωμάτων και φανερώθηκε η ροπή στον πολιτικό συγκεντρωτισμό και στον αντιδημοκρατισμό του πολιτικού συστήματος. Το ζήτημα της σύγκρουσης μεταξύ προστασίας των δικαιωμάτων των πολιτών και προάσπισης της «εθνικής ασφάλειας» είναι διαχρονικό, όπως και η καταχρηστική-διασταλτική ερμηνεία της έννοιας της «εθνικής ασφάλειας» από την εκάστοτε εξουσία.

Το ίδιο διαχρονική, όμως, είναι η συζήτηση γύρω από το τι συνιστά «κατάσταση εξαιρέσης» ενός κοινωνικοπολιτικού συστήματος και άρα «δικαιολογημένη» βάση συστολής των ατομικών δικαιωμάτων. Γιατί ο τρόπος χρήσης της έννοιας της «εθνικής ασφάλειας» στο γενικό νομικό πλαίσιο είναι μια κανονικοποιημένη «κατάσταση εξαιρέσης» με συνεπακόλουθη αδυναμία διαχωρισμού της από την «κανονικότητα» του δικαίου. Το αντίκτυπο της παραβίασης, εν τέλει, του επικοινωνιακού απορρήτου μέσω της μαζικής επιτήρησης και της γενικής συλλογής μεταδεδομένων, δεν αφορά μόνο την ιδιωτική ζωή,

αλλά ένα ευρύ φάσμα δικαιωμάτων σχεδόν σε κάθε πτυχή της ζωής μας, μαζί με την αυτονομία και την ελευθερία, τα οποία σχετίζονται με τη λειτουργία μας ως κοινωνία.

Βιβλιογραφία

1. Ξενόγλωσση βιβλιογραφία-αρθρογραφία

Al-Fedaghi, S., 2012. A Conceptual Foundation for the Shannon-Weaver Model of Communication. *International Journal of Soft Computing*, 19 12, p. 8.

Anon., 2018. Human Rights Judgment on Accessing IP Address Information. *Society for computers and law*, 23 April.

Bernal, P., 2016. Data gathering, surveillance and human rights: recasting the debate. *Journal of cyber policy* , 26 Αυγούστου, pp. 243-264.

Birrer A, Danya H., Just N., 2023. The state is watching you—A cross-national comparison of data retention in Europe. *Science Direct*, 4 April.

Bocos P. C, De Hert P., 2015. Case of Roman Zakharov v. Russia: the Strasbourg follow up to the Luxembourg court's Schrems judgment. *Strasbourg Observers*, 23 December.

Carrera S, Guild E, 2014. The Political and Judicial Life of Metadata:Digital Rights Ireland. *Liberty and Security*, May 29.

Chatzinikolaou, A., 2018. Benedik v. Slovenia: Police need a court order to access subscriber information associated with a dynamic ip address. *Strasburg Observers*, June.

Chia, A., 2023. Metadata 101: Definition, Types & Examples. *Splunk, A CISCO Company*, 22 June.

Christakis, T., 2018. Afragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch judgment. *European Law Blog*, 18 September.

Cole, D., 2014. 'We Kill People Based on Metadata'. *The New York Review*, 14 May.

Cooley, C. H., 1998. *On Self and Social Organization:edited with an introduction by Hans-Joachim Schubert*. Chicago: The University of Chicago Press.

Dimitrova, D., 2022. Ekimdzhev and others v. Bulgaria: secret surveillance and electronic communications surveillance only with adequate safeguards, or nothing new under the sun. *Strasburg Observers*, 2 March .

Erotokritou, C., 2022. Access Alert | New Judgments from the Court of Justice of the European Union on Data Retention by Providers of Electronic Communications. *Access Partnership* , 11 October.

Ferran, L., 2014. Ex-NSA Chief: 'We Kill People Based on Metadata'. *ABC News*, 12 May.

Fiske, J., 2011. *Introduction to Communication Studies*. 3rd edition ed. London: Routledge.

- Klamberg, M.**, 2021. Big Brother's Little, More Dangerous Brother. 1 June.
- Kosta, E.**, 2017. Surveilling masses and unveiling human rights. *Tilburg University*.
- Landau, S.**, 2020. Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy. *ACM Digital Library*
- Mayernik M. S., Acker A.**, 2018. Tracing the Traces: The Critical Role of Metadata Within Networked Communications. *Journal of the Association for Information Science and Technology, Volume 69, Issue 1, Opinion Paper, January*, pp. C1, 1-184.
- Mitrou L.**, 2007, *Communications Data Retention: A Pandora's Box for Rights and Liberties? Digital Privacy*, New York, Chapter 20
- Rovelli, S.**, 2021. Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention. *Europen Papers*, 11 June.
- Sajfert, J.**, 2021. The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?. *EUROPEAN LAW BLOG- News and comments on EU Law*, 8 June.
- Schade, H.**, 1985. International Law- The right to respect for private life. *The Cambridge Law Journal 44*, pp. 180-183.
- Statewatch**, 2022. Bulgaria: Secret surveillance data "could be used for nefarious purposes" due to lack of safeguards, rules ECHR. January.
- Timmer, E.**, 2024. ECHR judgment on Polish legislation on secret surveillance. *Ellen Timmer – juridische artikelen en berichten*, 8 July.
- Tomszewski, Z.**, 2003. *Fiske's Introduction to Communication Studies*. Paper 4 επιμ. s.l.:for CIS 701, taught by Maria Tehranian.
- Vermeulen, J.**, 2020. Bulk retention of private-sector subscriber data for governmental purposes does not violate the convention: Breyer v. Germany. *Strasbourg Observers*, 5 March.
- Vogiatzoglou, P.**, 2018. "Bulk interception of communications in Sweden meets convention standards": the latest addition to mass surveillance case law by the European court of human rights. *Strasbourg Observers*, 09 July.
- Watt, E.**, 2021. Much ado about mass surveillance – the ECTHR grand chamber 'opens the gates of an electronic "big brother" in Europe' in Big Brother Watch v. UK. *Strasbourg Observer*, 28 June.

2. Ελληνική βιβλιογραφία-αρθρογραφία

- Αλεξοπούλου, Κ.**, 2017. Προστασία του απορρήτου της επικοινωνίας στο πλαίσιο της ΕΣΔΑ. Στο: *Εφημερίδα Διοικητικού Δικαίου 4*. Αθήνα : Σάκκουλας, σελ. 14.
- Δήλωση 20 Καθηγητών του Συνταγματικού Δικαίου για την Γνωμοδότηση 1/2023 του Εισαγγελέα του Αρείου Πάγου**, 2023, *Constitutionalism, Ομιλος Αριστόβουλος Μάνεσης*, 12 Ιανουαρίου.

Διονυσοπούλου Α., 2022, Άρση απορρήτου τηλεφωνικής επικοινωνίας στον νέο Κώδικα Ποινικής Δικονομίας-Η σχέση των άρθρων 254-255 ΚΠΔ και του ν.2225/1994, *Ποινικά Χρονικά*

Κοντιάδης, Ξ., 2023. Η σύγκρουση Ανεξάρτητων Αρχών και πολιτικής εξουσίας: Εισήγηση στο Συνέδριο “Συνταγματικά κατοχυρωμένες Ανεξάρτητες Αρχές: Η συμβολή τους σε ένα ευρωπαϊκό δημοκρατικό κράτος δικαίου”. *Syntagma Watch*, 03 Νοεμβρίου.

Κοντιάδης, Ξ., 2024. Ο Ξενοφών Κοντιάδης σχολιάζει τον ρόλο της ΑΔΑΕ, μετά την απόφαση του ΣτΕ στην περίπτωση Ανδρουλάκη. *Syntagma watch*, 08 Απριλίου.

Κοντιάδης, Ξ., Σωτηρέλλης Γ., 2023. Τα πολλαπλά ατοπήματα της γνωμοδότησης του εισαγγελέα του Αρείου Πάγου σχετικά με τις αρμοδιότητες της ΑΔΑΕ, *Syntagma Watch*, 12 Ιανουαρίου.

Κουσουνή-Πανταζοπούλου Α., 2022, Οι πρόσφατες νομολογιακές εξελίξεις αναφορικά με τη γενική διατήρηση δεδομένων ηλεκτρονικών επικοινωνιών, *ΔΙΤΕ*, τεύχος 3/2022.

Κρουστάλλη, Δ., 2024. Υποκλοπές: Τι σημαίνει η απόφαση του ΣτΕ. *ΤΟ ΒΗΜΑ*, 05 Απριλίου.

Λίβος Ν., 1997 Η προστασία των συνδυασμένων δεδομένων των τηλεπικοινωνιών, *ΠοινΧρ (ΜΖ')* σελ. 747 επ.

Μακρής, Σ., 2023. Το Predator και τα προσωπικά δεδομένα. Οι πολλαπλές παραβιάσεις της εθνικής και ευρωπαϊκής νομοθεσίας και τα πρακτικά και νομικά προβλήματα για την εφαρμογή της. Ομιλος “Αριστόβουλος Μάνεσης”, 10 Φεβρουαρίου.

Μαντζούφας Π.,2024. Το συνταγματικό πλαίσιο του δικαιώματος επικοινωνίας και οι προϋποθέσεις άρσης του απορρήτου για λόγους εθνικής ασφάλειας, *Constitutionalism*, 21 Σεπτεμβρίου.

Μαυριάς, Κ., 1982. *Το συνταγματικό δικαίωμα ιδιωτικού βίου*. εκδ.:ΑΝΤ. Ν. ΣΑΚΚΟΥΛΑΣ.

Μποτόπουλος, Κ., 2024. Συμβούλιο της Επικρατείας και «απόφαση Ανδρουλάκη». *Syntagma Watch*, 09 Απριλίου.

Παλαμιώτης Φ., Παπατόλιας Α., 2022. «Το Σύνταγμα στη δίνη των υποκλοπών». Συνταγματικές και δικαιο-πολιτικές όψεις της υπόθεσης των παρακολουθήσεων», *Constitutionalism*.

Παναγοπούλου, Φ., 2023. Άρθρο 19. ΣΥΝΤΑΓΜΑ, *Ερμηνεία κατ’ άρθρο*, Επιμ: Σπ. Βλαχόπουλος, Ξεν. Κοντιάδης, Γ. Τασόπουλος. Αθήνα: Κέντρο Ευρωπαϊκού Συνταγματικού Δικαίου, *Syntagma Watch*.

Παπαδόπουλος, Ν. Κ., 2008. *Προστασία του απορρήτου της επικοινωνίας*. Αθήνα: Νομική Βιβλιοθήκη.

Παπανικολάου, Αι., 2020. Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα. 22 Ιουλίου.

Παπανικολάου Αι., 2022. Έλλειμμα διαφάνειας και λογοδοσίας, *Η ΚΑΘΗΜΕΡΙΝΗ*, 14 Αυγούστου

Παπανικολάου, Αι., 2022. Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών, *Syntagma Watch*, 31 Αυγούστου

Παπασπύρος, Ν., 2023. Οι αρμοδιότητες της ΑΔΑΕ και το κράτος δικαίου, *constitutionalism*.

Παπατόλιας Α.Ι., 2022, Τα όρια του κοινοβουλευτικού ελέγχου των παρακολουθήσεων, *constitutionalism*.

Πρεβεδούρου, Ε. Β., 2024. Σύνθεση Δημοσίου Δικαίου: Νέα περίπτωση εφαρμογής της έννοιας του “επαυξημένου Συντάγματος”: η απόφαση ΣτΕ Ολ 465/2024 (22-04-2024). 22 Απρίλιος.

Ράμμος Χ., Γκριτζαλης Σ. & Παπανικολάου Α., 2021. Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών, *Constitutionalism*

Σουλιώτης, Γ., 2024. ι εκάστοτε εποπτεύοντες εισαγγελείς δεν τηρούν φακέλους υποθέσεων και ως εκ τούτου ο ίδιος δεν έχει πρόσβαση στον φάκελο της παρακολούθησης του προέδρου του ΠΑΣΟΚ Νίκου Ανδρουλάκη.. *Η Καθημερινή*, 15 Μαΐου.

Συμεωνίδου-Καστανίδου, Ε., 2022. Το σχέδιο νόμου σχετικά με την άρση του απορρήτου των επικοινωνιών: κρίσιμες για τις θεμελιώδεις ελευθερίες «αστοχίες». *Constitutionalism-Ομιλος Αριστόβουλος Μάνεσης*.

Σωτηρέλης, Γ. Χ., 2023. Συνταγματική αποτίμηση και θεσμικές προεκτάσεις της ομόθυμης καταδίκης της γνωμοδότησης Ντογιάκου. *Constitutionalism-Ομιλος Αριστόβουλος Μάνεσης*, 16 Ιανουαρίου.

Τασόπουλος Γ. 2023. Προιονίζοντας τα συνταγματικά θεμέλια των Ανεξάρτητων Αρχών, *Syntagma Watch*, 1 Νοεμβρίου

Τελόγλου Τ, Τριανταφύλλου Ε., 2022. «Ποιος παρακολουθούσε το κινητό του δημοσιογράφου Θανάση Κουκάκη;». *Inside Story*, 4 Ιανουαρίου.

Τσίρης, Π., 2002. *Η Συνταγματική κατοχύρωση του δικαιώματος του απορρήτου της επικοινωνίας*. Αθήνα: Σάκκουλας.

Τσόλιας, Γ., 2016, ΣτΕ 1593/2016 (Τμ. Δ) (Τηλεπικοινωνίες. Απόρρητο)». *ΔΙΤΕ (π. ΔΙΜΕΕ) (Τεύχος 4/2016)*.

Τσόλιας, Γ., 2017, Δ.Ε.Ε. υποθ. C-203/2015, C-698/2015 απόφ. της 21.12.2016 [Δεδομένα προσωπικού χαρακτήρα και ηλεκτρονικές επικοινωνίες *ΔΙΤΕ (π. ΔΙΜΕΕ) (Τεύχος 1/2017)*.

Τσόλιας, Γ., 2021. Άρθρο 8 (συνέχεια)- Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής (Απόρρητο της επικοινωνίας). Στο: *Ι. Σαρμάς/Ξ. Κοντιάδης/Χ.Αθανασόπουλος, ΕΣΔΑ Κατ'άρθρον ερμηνεία*. Αθήνα-Θεσσαλονίκη: Σάκκουλα, σελ. 25.

Τσόλιας, Γ., 2023. Το νομικό πλαίσιο άρσης του απορρήτου των ηλεκτρονικών επικοινωνιών για την διακρίβωση εγκλημάτων σύμφωνα με τις διατάξεις του Ν 5002/2022 και η απωλεσθείσα ευκαιρία εκσυγχρονισμού του. *Ποινική Δικαιοσύνη*, Issue 03.

Φωτιάδου Α, Παπανικολάου, Αι., 2022. Αναδημοσίευση: Προβλήματα κατά την άρση απορρήτου των επικοινωνιών – Συνέντευξη της Δρ. Αικατερίνας Παπανικολάου, μέλους της ΑΔΑΕ, *Syntagma Watch*, 30 Αυγούστου

Χονδρόγιαννος, Θ., 2022. Παρακολούθηση του Νίκου Ανδρουλάκη από την ΕΥΠ. *Govwatch*, 26 Σεπτεμβρίου.

Χρυσόγοννος, Κ. 2022. Το απόρρητο της επικοινωνίας και το πρόβλημα της δημοκρατικής ποιότητας του πολιτεύματος, *Constitutionalism*.

Χρυσόγοννος, Κ., 2023. Το άρθρο 19 του Συντάγματος υπό την σκιά του “Μεγάλου Αδελφού”. Ο ν. 5002/2022 και η 1/2023 γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου. *Ομιλος Αριστόβουλος Μάνεσης*, 20 Ιανουαρίου.

3. Κανονισμοί και Οδηγίες της ΕΕ

Proposal for a *Regulation of the European parliament and of the council* concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (**Regulation on Privacy and Electronic Communications**), 2017/003 COD, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

Regulation (EU) 2016/679 on Privacy and Electronic Communications (GDPR), Διαθέσιμο σε: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Οδηγία 2002/58/ΕΚ, Διαθέσιμη σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058>

4. Αποφάσεις ΕΔΔΑ

Iordachi and Others v. Moldova, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-91245%22%5D%7D>

Malone v. The United Kingdom, Διαθέσιμο σε: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57532%22%5D%7D>

Roman Zakharov v. Russia, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-159324%22%5D%7D>

Szabó and Vissy v. Hungary, Διαθέσιμο σε: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-160020%22%5D%7D>

Centrum för Rättvisa v. Sweden, Διαθέσιμο σε:

[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-210078%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210078%22]})

Big Brother Watch and others v. UK, Διαθέσιμο σε:

[https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-210077%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]})

Benedik κατά Σλοβενίας, Διαθέσιμο σε:

[https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22benedik%22\],%22documentcollectionid2%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-182455%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22benedik%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-182455%22]})

Breyer

κατά

Γερμανίας,

Διαθέσιμο

σε:

[https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-200442%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200442%22]})

Ekimidzhiev κατά Βουλγαρίας, Διαθέσιμο σε: <https://www.statewatch.org/media/3031/bg-echr-secret-surveillance-aip-legal-summary-11-01-22.pdf>

Pietrzak and Bychawska-Siniarska and Others v. Poland Legal Summary, Διαθέσιμο σε:

[https://hudoc.echr.coe.int/eng#{%22languageisocode%22:\[%22ENG%22\],%22appno%22:\[%2272038/17%22,%2225237/18%22\],%22documentcollectionid2%22:\[%22CLIN%22\],%22itemid%22:\[%22002-14333%22\]}](https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%2272038/17%22,%2225237/18%22],%22documentcollectionid2%22:[%22CLIN%22],%22itemid%22:[%22002-14333%22]})

5. Αποφάσεις ΔΕΕ

Digital Rights Ireland και άλλοι, Διαθέσιμο σε:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=162437&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=19628265>

Tele2 Sverige AB (C 203/15) κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis, Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0203>

Prokuratuur C-746/18, Διαθέσιμο σε:

<https://curia.europa.eu/juris/liste.jsf?language=en&num=c-746/18>

Joined Cases C-339/20 (VD) and C-397/20(SR) και Joined Cases C-793/19 (SpaceNet) and C-794/19 (Telekom Deutschland), Διαθέσιμο σε:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=265882&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1193073>

6. Ιστοσελίδες-Blog

Article 19, 2024. European Court of Human Rights: Important decision against mass surveillance. 28 May. Διαθέσιμο σε: <https://www.article19.org/resources/european-court-of-human-rights-important-decision-against-mass-surveillance/>

Big Blue Data Academy, «Τι Είναι τα Μεταδεδομένα (Metadata): Σημασία, Τύποι & Χρήσεις», Big Blue Data Academy, 01 Δεκεμβρίου 2023, Διαθέσιμο σε: <https://bigblue.academy/gr/metadedomena>

Global Freedom of Expression, 2016. Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson. *Global Freedom of Expression*, Columbia University. Διαθέσιμο σε: <https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/>

GDPR HUB, CJEU - C 203/15 and C 698/15 - Tele2/Watson (Joined Cases) Διαθέσιμο σε: [https://gdprhub.eu/index.php?title=CJEU - C 203/15 and C 698/15 - Tele2/Watson \(Joined Cases\)](https://gdprhub.eu/index.php?title=CJEU - C 203/15 and C 698/15 - Tele2/Watson (Joined Cases))

ICO, Διαθέσιμο σε: <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/communications-networks-and-services/traffic-data/#trafficdata>

Pila, 2024. European Court of Human Rights Rules Polish “Secret-Surveillance Regime” Violates European Convention on Human Rights. *Pila*, 05 June, Διαθέσιμο σε: <https://www.pila.ie/resources/bulletin/2024/06/05/european-court-of-human-rights-rules-polish-secretsurveillance-regime-violates-european-convention-on-human-rights>

Privacy International, 2024. Pietrzak and others v Poland. *Privacy International*. Διαθέσιμο σε: <https://privacyinternational.org/legal-action/pietrzak-and-others-v-poland>

Privacy International, Szabo v. Hungary (Hungary Mass Surveillance). *Privacy International*. Διαθέσιμο σε: <https://privacyinternational.org/legal-action/szabo-v-hungary-hungary-mass-surveillance>

Society for Computers and Law, 2018: <https://www.scl.org/10201-human-rights-judgment-on-accessing-ip-address-information/>

Written submissions on behalf of Privacy International and Article 19, Διαθέσιμο σε: <https://privacyinternational.org/taxonomy/term/407>

7. Δελτία τύπου ΑΔΑΕ

ΑΔΑΕ Δελτίο Τύπου - Περίληψη των πλέον σημαντικών παρατηρήσεων επί του νομοσχεδίου για την διαδικασία άρσης απορρήτου των Επικοινωνιών, την κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων, 2022, Ανακτήθηκε από: <https://adae.gov.gr/enimerosi/deltia-typou/perilepseton-pleon-semantikon-paratereseon-epi-tou-nomoschediou-gia-ten-diadikasia-arses-aporretou-ton-epikoinonion-ten-kybernoasphaleia-kai-ten-prostasia-prosopikon-dedomenon>

ΑΔΑΕ Δελτίο Τύπου-Απόφαση , 24/04/2024, Διαθέσιμο σε: <https://adae.gov.gr/enimerosi/deltia-typou/deltio-typou-apophase-tes-adae>

8. Γνωμοδοτήσεις

Article 29 Data Protection Working Party, 2017, Διαθέσιμο σε: http://ec.europa.eu/justice/data-protection/index_en.htm

EDPS, 2017, Opinion 6/2017, Διαθέσιμη σε:

https://edps.europa.eu/sites/edp/files/publication/17-04-24_privacy_en.pdf

Council of the European Union, Judgment of the Court of 8 April 2014 and invalidation of the Directive 2006/24, 9009/14, 5 May 2014, Brussels, Διαθέσιμο σε:

<https://www.statewatch.org/media/documents/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf#page=1.63>

Γνωμοδότηση 9/2009, Διαθέσιμη σε:

<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-09-2009/>

Γνωμοδότηση 19/2009, Διαθέσιμη σε:

<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-12-2009/>

Γνωμοδότηση 9/2011, Διαθέσιμη σε:

<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-09-2011/>

ΑΔΑΕ Γνωμοδότηση 1/2005, Διαθέσιμη σε: <https://adae.gov.gr/images/nomothetiko-plaisio/893-2005.pdf>

Γνωμοδότηση 1/2023 Εισαγγελία Αρείου Πάγου, Διαθέσιμη σε:

<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-1-2023/>

9. Διεθνή κείμενα

Electronic Communications Privacy Act of 1986 (ECPA), Bureau of Justice Assistance, US

Department of Justice, Διαθέσιμο σε: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#1-0>

In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc., No. BR 13- 80 (FISC Apr. 25, 2013), Διαθέσιμο σε:

<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-059.pdf>

10. Podcast

Συναντήσεις στο Σύνταγμα Ε11: Οι Ανεξάρτητες Αρχές σε κρίσιμη καμπή, 2023. *Syntagma Watch*, 19 Οκτωβρίου, Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/podcast-synantiseis-sto-syntagma-ep-11-oi-anexartites-arhes-se-krisimh-kamph/?fbclid=IwY2xjawFmqQpleHRuA2FlbQIxMQABHTZ-6KxJ9cwWK0dMheGZMblz3Fq0uU-wxliccG7B1fKswNlfnCZvUqZHA_aem_9I9zjURgtwXHI1PaBVyf_Q